S. HRG. 98-228

CREDIT CARD FRAUD

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER AFFAIRS

OF THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

UNITED STATES SENATE

NINETY-EIGHTH CONGRESS

FIRST SESSION

ON

ISSUES CAUSED BY RISING CREDIT CARD FRAUD, TO DETERMINE WHETHER THE TRUTH-IN-LENDING ACT AND THE ELECTRONIC FUND TRANSFER ACT ADEQUATELY PROTECT CONSUMERS AND INSTITUTIONS FROM FRAUD AND ABUSE, AND TO CONSIDER POTENTIAL LEGISLATIVE REMEDIES

MAY 18, 1983

Printed for the use of the
Committee on Banking, Housing, and Urban Affairs

U.S. GOVERNMENT PRINTING OFFICE
22-429 O WASHINGTON : 1983

S241-34

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

JAKE GARN, Utah, *Chairman*

JOHN TOWER, Texas
JOHN HEINZ, Pennsylvania
WILLIAM L. ARMSTRONG, Colorado
ALFONSE M. D'AMATO, New York
SLADE GORTON, Washington
PAULA HAWKINS, Florida
MACK MATTINGLY, Georgia
CHIC HECHT, Nevada
PAUL TRIBLE, Virginia

WILLIAM PROXMIRE, Wisconsin
ALAN CRANSTON, California
DONALD W. RIEGLE, Jr., Michigan
PAUL S. SARBANES, Maryland
CHRISTOPHER J. DODD, Connecticut
ALAN J. DIXON, Illinois
JIM SASSER, Tennessee
FRANK R. LAUTENBERG, New Jersey

M. Danny Wall, *Staff Director*
Kenneth A. McLean, *Minority Staff Director*

Subcommittee on Consumer Affairs

PAULA HAWKINS, Florida, *Chairman*

ALFONSE M. D'AMATO, New York
SLADE GORTON, Washington

CHRISTOPHER J. DODD, Connecticut
ALAN J. DIXON, Illinois

Beth L. Climo, *Senior Counsel*
Pat Abshire, *Legislative Assistant*
Charles L. Marinaccio, *Minority General Counsel*

CONTENTS

WEDNESDAY, MAY 18, 1983

Page

Opening statement of Senator Hawkins 1
Opening statement of Senator D'Amato 9

WITNESSES

James Knapp, Deputy Assistant Attorney General, Criminal Division, Department of Justice, accompanied by Donald Foster, Deputy Chief, Fraud Section, Criminal Division, Department of Justice 3
  Prepared statement 3
Charles P. Nelson, Assistant Chief Postal Inspector for Criminal Investigation, U.S. Postal Service, accompanied by Wayne Kidd, Postal Inspector 6
  Prepared statement 7
  Response to Senator Proxmire request for cost of making a credit card counterfeit-proof 16

Panel discussion:

  Amend existing statutes 11
  "White collar crimes" 11
  Organized credit card fraud 12
  Credit card losses exceed bank robberies 13
  Operation of counterfeit cards 18
  Criminal penalties not stiff enough 20
  Investigation and prosecution has not been extensive 22
John G. Alexander, senior vice president, Bank One of Columbus, Columbus, Ohio, chairman, American Bankers Association, Task Force on Credit Card Fraud 25
  Prepared statement 25
    Industry efforts 25
    Need for legislation 26
    Safeguarding the account number 27
    Conclusion 28
    Appendix A—Credit card industry total fraud losses 29
    Appendix B—Draft of a bill to amend the Truth-in-Lending Act and the Electronic Fund Transfer Act 30
James R. Branam, Jr., senior vice president, Southeast Services, Inc., Miami, Fla., on behalf of Florida Bankers Association 31
  Prepared statement 32
    Links to narcotics and other illegal activities 32
    Schemes and scams 32
    White plastic 33
    Consumer abuses 33
    Summary 34
William Neuman, vice president for security, VISA International 34
  The scope of the problem 34
  How fraud is perpetrated 35
  Congressional action needed 36
  Account number information dissemination 37
  Conclusion 37
  Prepared statement 39
Thomas Kelleher, vice president for security, MasterCard International 82
  Fraud losses grow unspectacularly 82
  Organized crime, violence associated with account abuses 84

Thomas Kelleher, vice president for security, MasterCard International—Continued
Page
  Loopholes in existing legislation 85
  Prepared statement 87
    Appendix A:
      Fraud losses reported 102
      Counterfeit losses reported 102
    Appendix B:
      Draft of a bill to amend the Truth-in-Lending Act and the Electronic Fund Transfer Act 104
      Draft to add a new chapter to title XVIII to proscribe various activities in connection with payment devices 107
Panel discussion:
  Research for counterfeit-proof credit cards 117
  Using carbonless copies of credit card slips 119
  Sales of lists with account numbers 120
Milton Schober, Esq., on behalf of American Retail Federation 123
  Urge caution in approaching legislation 123
  Hot card lists 124
  Prepared statement 126
Walter R. Kurth, president, Associated Credit Bureaus, Houston, Tex 130
  Prepared statement 130
John Baker, president, the Credit Bureau, Inc., accompanied by Brian Garrett 132
  Prepared statement 133
    CBI 133
    Credit fraud and security procedures 135
    Legitimate uses of account numbers 136
    Conclusion 141
    Summary of rights provided by the Fair Credit Reporting Act and CBI's fair information practices 144
William B. Price, president, CBC Cos., Inc., Columbus, Ohio 146
  Prepared statement 147
Panel discussion:
  Improvement in the verification process 150
  Impact of prohibition on the sale and distribution of lists 150

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Consumer Affairs Office of Palm Beach County, testimony of Alice C. Skaggs, director, with sworn statements and complaints of consumers 151
National Retail Merchants Association, statement submitted for the record 161

CREDIT CARD FRAUD

WEDNESDAY, MAY 18, 1983

U.S. Senate,
Committee on Banking, Housing, and Urban Affairs,
Subcommittee on Consumer Affairs,
Washington, D.C.

The subcommittee met at 10 a.m. in room SD-538, of the Dirksen Senate Office Building, Paula Hawkins (chairman of the subcommittee) presiding.

Present: Senators Hawkins, D'Amato, Proxmire, and Dodd.

OPENING STATEMENT OF SENATOR HAWKINS

Senator **Hawkins**. The subcommittee will come to order.

We have a long hearing today and we're going to ask in the interest of time that the witnesses condense their statement to a summary of around 5 minutes. Senator D'Amato is on his way and will have questions for you. We will enter your full statement in the record. We do have a lot of questions for you.

The Consumer Affairs Subcommittee of the Senate Banking Committee is holding these hearings today to explore issues caused by rising credit card fraud, especially its impact on the cost and availability of consumer credit. In addition, one purpose of the hearing is to determine whether the two principal statutes addressing the problem, the Truth-in-Lending Act and the Electronic Fund Transfer Act, adequately protect consumers, and the institutions that issue credit and debit cards, from fraud and abuse.

On a related matter, we will also investigate and consider potential legislative remedies, concerning allegations that some companies selling credit card protection services bill customers who elect not to buy the services.

Credit card fraud, which can take many different forms, is growing rapidly and now exceeds $1 billion a year. One form of fraud involves counterfeiting. Losses due to counterfeiting in the worldwide credit industry were estimated at $50 million in 1982, up from $15 million in 1981, a staggering increase. Counterfeit losses involving VISA cards alone were $10 million in 1982, 15 times greater than the previous year, and 7 times greater than the total counterfeit losses for the previous 9 years.

Available statistics indicate that New York and Florida lead in credit card counterfeiting. For example, VISA International suffered 42.7 percent of its total U.S. counterfeit losses in New York and 19.1 percent in Florida.

In some Florida cases preimprinted sales drafts were used; in others, cards only with numbers on them called "white plastics."

From intelligence reports, it is apparent that major criminal organizations are involved.

On January 5, 1980, postal authorities arrested a New York mobster at a Miami hotel with preimprinted sales drafts. The defendants stated that they had processed $12,000 worth of sales drafts for 20 days for a total of $240,000.

The Plantation, Fla., Police Department in May 1982 seized a Ryder rental truck that was obtained with an altered credit card from department stores in Tampa, Fla. As a result of this seizure, a search warrant was executed, and an embosser was seized. This embosser was one of two that were purchased in New Rochelle, N.Y., by a suspected member of a crime organization. The other embosser was seized in an arrest of a suspect in Los Angeles, Calif., where 139 altered cards were found. Similar reports indicate that the counterfeit problems facing New York and Florida are spreading to other areas.

Another form of fraud involves false billing by merchants who first acquire credit card numbers through ordinary transactions then process others that did not take place. The potential for danger is apparent from the following example. In May 1982, a merchant in Sunrise, Fla., attempted to deposit $24,000 in fraudulent sales drafts. This transaction was halted by an alert bank teller and her manager. In other cases, merchants or their employees pass on to others carbon copies of charge slips. These slips are then used to generate false documentation for phony transactions.

These are just a few examples of credit card scams operating in Florida and other States, but one thing is clear; fraud involves more than lost or stolen credit cards. The witnesses today will tell us about other cases.

Rising credit card fraud affects each of us daily, not just those who are its direct victims. It is true that financial institutions that issue cards and merchants who accept them without following authorization procedures bear the immediate costs. That is because cardholder's liability when his card is used fraudulently is usually limited to $50 per card. However, these losses are passed back to cardholders and consumers eventually, as a component of the cost of credit and merchandise. Thus, we all pay.

The hearing will also address the misuse of credit card holder identification numbers. In Sarasota, a Florida credit card protection firm has been accused by more than 3,000 south Florida consumers of making unauthorized charges on their VISA cards and MasterCards. For a fee, credit card protection services keep a list of their clients' credit card account numbers with the promise to notify the card issuers if any of their credit cards are lost or stolen. The firm in question blitzed the Sarasota area with solicitations for its services and, according to a cease-and-desist order issued by the Florida attorney general the firm levied unauthorized charges through their credit card accounts on consumers who turned them down. The unauthorized charges apparently were made possible by the firm because it had acquired a list of account holders' names and account numbers.

This abusive practice was called to my attention by Alice Skaggs, director of the Consumer Affairs Office of West Palm Beach. Mrs. Skaggs was scheduled to appear at these hearings to elaborate on this problem, but unfortunately has been prevented from coming to Washington. I will submit her written testimony for the record.

(See p. 151.)

I'm considering introducing legislation to meet this problem by restricting the dissemination of credit card holder lists and account numbers.

In addition, because we are considering legislation to restrict the dissemination of credit card holder lists and account numbers, we will be interested in hearing what witnesses consider to be legitimate uses of these lists by business firms and financial institutions.

I am particularly interested in determining the extent to which organized crime syndicates operate credit card fraud rackets and whether there is a connection between trafficking in illegal drugs and counterfeit credit cards.

The witnesses appearing today will help indicate the magnitude of these problems and, I anticipate, will suggest ways we can better protect both consumers and card issuers from credit card fraud and abuse. We welcome comments on legislative solutions. One of our witnesses has just called and he's still on an airplane on his way here. We hope he will arrive in time to testify.

The first panel consists of Mr. James Knapp, Deputy Assistant Attorney General, Criminal Division, Department of Justice; and Mr. Charles P. Nelson, Assistant Chief Postal Inspector for Criminal Investigation, U.S. Postal Service. We welcome you here today and look forward to your testimony.

STATEMENT OF JAMES KNAPP, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, ACCOMPANIED BY DONALD FOSTER, DEPUTY CHIEF, FRAUD SECTION, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE.

Mr. **Knapp**. Thank you, Senator.

[Complete statement follows:]

Statement of James Knapp, Deputy Assistant Attorney General, Criminal Division

Madam Chairman and members of the subcommittee, I am pleased to be here to discuss the magnitude of credit and debit card fraud and the adequacy of protection afforded by the Truth-in-Lending Act and the Electronic Funds Transfer Act for consumers and issuers of credit and debit cards. With me today is Donald W. Foster, Deputy Chief of the Fraud Section of the Criminal Division. We will be looking at the criminal fraud provisions of the Truth-in-Lending Act, 15 U.S.C. 1644, and the criminal fraud provisions of the Electronic Funds Transfer Act, 15 U.S.C. 1693n. We will also look at the present and proposed statutes that are germane to the problem of credit and debit card fraud.

Our basis conclusion is that no significant changes are needed with the provisions of these two statutes other than to clarify two problems which have arisen as a result of case law decisions and to broaden their coverage to include counterfeiting and altering of credit cards. We also support changes in the Right to Financial Privacy Act, 12 U.S.C. 3401, et. seq., and a proposal, pending before the Congress in the President's Crime Bill, S. 829.

Criminal Division and Federal Bureau of Investigation officials have been meeting with bank and bank card industry representatives on this issue since July 1982. Thus, we are aware of the dramatic increase in counterfeit and fraud activity in the credit card area. We are also aware of the dramatic increase in Electronic Fund Transfer [EFT] activity through a preliminary study done by the Department's Bureau of Justice Statistics in June 1982, and our conversations with the industry representatives. The industry statistics clearly show the increase in credit card fraud: losses in 1981 and 1982 were nine times as great as the total for the past 7 years; and the annual loss to the banking community through credit card fraud is far in excess of the proceeds of bank robberies (some $128 million vs. $46.8 million in 1982). Similarly, we realize that the increased numbers of EFT systems and the proliferation of debit cards creates the possibility for the same rapid rise in losses. Since the first Automatic Teller Machine [ATM] was installed in 1970, there are now approximately 26,000 units, each processing an average of 7,000 transactions per month. There are about 50 million debit cards in circulation, triple the number 2 years ago and almost equal to the domestic circulation of VISA credit cards. We further understand that with ATM network sharing the volume is expected to continue to expand even more dramatically and ATMs are only one of the five principal EFT systems.

Our concern in this area, however, is not with the high volume, low dollar losses of present or future credit or debit card transactions. The average credit or debit card fraud loss is small and can be prosecuted on a local level if prosecution is warranted.

The Federal investigation and prosecution effort has not been extensive. The Postal Inspection Service, according to our information, investigated 80 credit card frauds in 1982. The Federal Bureau of Investigation, with separate statistics available on EFT investigations only from October 1, 1982, have investigated nine cases since then. There have been only minimal federal prosecutions using the credit card statute, 15 U.S.C. 1644, and one using the EFT statute, 15 U.S.C. 1693n. There are, as I indicated, far more State and local prosecutions since credit card fraud is traditionally an area handled on a local basis.

These problems, do not, however, mandate a wholesale revision as contemplated in draft bills we have seen prepared by the banking and credit card industry. Some of these bills would involve the Federal Government in traditional areas of exclusively local interest by making virtually every credit card offense a federal offense. Some remove the $500 and $1,000 dollar limitations in the amount of loss contained in present law. Since the average ATM transaction in 1982 was only $47 and the average crime only $265, State prosecution is more appropriate. The high volume, low dollar loss situation is consistent with the use of State prosecution where personnel resources are greater by far.

The Department of Justice has been working more closely than ever before with State attorneys general and local district attorneys through our executive working group of Federal, State, and local prosecutors on a national level and the Law Enforcement Coordinating Committees on a State and local level. After discussing some of the changes the bank and bank card representatives are seeking with state and local prosecutors, we have learned that they are uniformly opposed to any intrusion into this area of traditionally local concern.

Before the criminal sanctions are made more stringent, we strongly believe that card issuers need to do more to protect themselves. For a number of years the credit card issuers provided cards for any and everyone to attract business. Although they say now that they realize the error of their ways and should have had a more selective application and approval process, we see the same type of phenomenon in the tripling of debit cards in 2 years. Further, counterfeiting and unauthorized access to account information is indeed a problem for the industry, but it is in large part due to the lack of security built into the cards and the internal systems. We would prefer that the credit card and EFT industry leaders continue to improve the integrity of their own systems.

The Department is more concerned about the problem of counterfeiting and altering credit and debit cards. A number of investigations, Federal and local, have shown that there exists a substantial problem with organized criminal activity; not traditional Organized Crime, but ring activity of people associated together to commit a variety of crimes. The easy availability of false identification and the sophisticated techniques used in counterfeiting and altering cards makes it very easy for such groups to commit these types of crimes to support other criminal activity. We could support the amendment of the two statutes to cover counterfeiting and altering of the account numbers.

The Federal prosecutions in the credit card area do reveal certain defects in the Truth-in-Lending Act credit card statute that could be corrected. The Ninth Circuit Court of Appeals held in 1982 that the communication by telephone between Spokane, Washington, and Reno, Nevada, of fraudulently obtained credit card account numbers is not covered by the statute [*United States* v. *Callihan*, 666 F. 2d 422 (9th Cir. 1982)]. However, the court also held that the conviction under the wire fraud statute, 18 U.S.C. 1343, for transmitting the account number information was valid. As you are aware, had the telephone call not crossed state lines and thereby affected interstate commerce, the wire fraud statute would not have been applicable. The credit card statute could, therefore, be amended to include the fraudulent use of account numbers and information alone rather than the entire plastic card itself.

Other cases have highlighted a problem area with the statutory phrase "fraudulently obtained." Credit cards may be obtained by the original cardholder without an intent to defraud. They may later be sold or given to a defendant with the knowledge that the defendant would use the card to charge purchases without paying for them. Then the cards may be reported stolen or lost by the original cardholder. Under the present credit card statute, the cards are not "fraudulently obtained" within the meaning of the statute. Title 15 U.S.C. 1644 could therefore be amended to include transferring or obtaining a credit card as part of a scheme to defraud.

Since the EFT statute, 15 U.S.C. 1693n, parallels the credit card statute almost word-for-word, it also could be amended in these two respects.

To the extent that the subcommittee is reviewing Federal statutes affecting the ability of the Federal Government to investigate and prosecute fraud against financial institutions and other credit card issuers, I would invite your attention to the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401, et seq. That statute impedes Federal law enforcement efforts directed at crimes against financial institutions [which term embraces credit and debit card issuers, 12 U.S.C. 3401(1)] by prohibiting such institutions from disclosing financial records evidencing a fraud scheme except pursuant to legal process. Thus, a financial institution that has been defrauded cannot report the offense to Federal law enforcement officials complete with copies of financial records evidencing the crime. Rather, they must engage in the game of "Twenty Questions" with the Federal Bureau of Investigation in an effort to provide us with sufficient information to enable Federal officials to establish the basis for issuance of a grand jury subpoena or other form of legal process necessary to secure access to the records that evidence the crime. The Financial Privacy Act also restrains the ability of Federal bank supervisory agencies to transfer information relating to criminal activity to the Department of Justice.

In short, financial institutions are severely restricted by the Financial Privacy Act in their ability to report crimes, even when the financial institutions are themselves the victims. Any mistake by a financial institution in reporting a crime to Federal authorities exposes the institution to potential civil liability under 12 U.S.C. 3417. Moreover, any technical defect in a disclosure of records by a victimized financial institution entitles the fraud perpetrator to liquidated damages against the institution without regard to whether he was guilty of defrauding the bank. From a law enforcement perspective, it seems incredible that a financial institution could be punished civilly for reporting a crime against itself, yet this is the law today in the United States.

I would also like to comment briefly on a pending legislative item that impacts on the Credit Card and EFT Acts. It is contained in the President's Comprehensive Crime Control Act of 1983, S. 829, title XV, part H, section 1508. Present laws designed to protect banks cover the offenses of embezzlement, robbery, larceny, burglary, and false statements. The proposed statute is designed to fill the gaps in the present law regarding defrauding banks. It is modeled on the present mail and wire fraud statutes and proscribes a scheme or artifice to defraud a federally chartered or insured financial institution or to obtain property owned or under the custody or control of such an institution by means of false or fraudulent pretenses, representatives, or promises.

In conclusion, let me summarize our position. We support a tightening of the EFT and Truth-in-Lending statutes since case law has demonstrated a need to include account numbers and information within the definition of credit card and to expand the covered acts to obtaining or transferring cards as a part of a scheme to defraud. We support an expansion of both statutes to provide protection against counterfeiting and alteration. We support the President's comprehensive crime control bill that will fill in a gap in extisting law on schemes and artifices to defraud banks.

However, we do not support lowering existing minimum dollar loss requirements for Federal jurisdiction. Ordinary credit card fraud is an area of local concern, traditionally addressed by state and local prosecutors. Existing Federal law is adequate.

Thank you for this time. We will be pleased to answer any questions.

Senator **Hawkins**. Thank you, Mr. Knapp.

We'll call Mr. Nelson to give a summary of his testimony and then ask questions of the witnesses.

I recognize Senator Proxmire who has joined us. Do you have a statement?

Senator **Proxmire**. No.

STATEMENT OF CHARLES P. NELSON, ASSISTANT CHIEF POSTAL INSPECTOR FOR CRIMINAL INVESTIGATION, U.S. POSTAL SERVICE, ACCOMPANIED BY WAYNE KIDD, POSTAL INSPECTOR

Mr. **Nelson**. Thank you, Senator. As you covered earlier, we have submitted our formal testimony, and I will just read a summary of that testimony.

On my left is Postal Inspector Wayne Kidd. Mr. Kidd manages our fraud branch at headquarters.

The growth in the credit card industry in the late sixties led to a corresponding growth in credit card fraud along with an increase in our investigative activity in this area.

In addition to responding to the industry's problems through an aggressive investigative effort, we strongly urged and encouraged the creation and expansion of the security and investigative efforts within the industry.

During the 1960's and 1970's many successful prosecutions were obtained under the mail fraud statute. The highest volume of mail fraud cases involving credit card offenses was in 1972 when we investigated over 2,000 such incidents. These were usually relatively simple cases compared with the more complex ones we investigate today.

This changed dramatically on January 8, 1974, when the U.S. Supreme Court, in a 5-to-4 decision, affirmed a Sixth Circuit Court of Appeals decision in *United States* v. *Maze*. 414 U.S. 395 (1974). Following this decision, the number of mail fraud credit card investigations decreased significantly. Our investigations do not provide us any way of knowing how much credit card fraud there is in terms of dollars and cents. Such a figure can only be obtained from the industry itself.

It should be remembered that by no means do we investigate all instances of credit card misuse. The Postal Inspection Service is no more able to police the credit card industry than it is to police the insurance or the "cents-off" coupon industry. Law enforcement can only attempt to deal with some of the manifestations of the problem. It is not the total solution.

As we see it, a major problem now facing the bank card industry is counterfeit cards and schemes using account numbers without cards. The industry itself must continue to identify and aggressively pursue the latest technological advances in security to ensure that its cards and the system are protected from fraud and abuse. Preventive measures to reduce or eliminate such activity are essential in order to preserve the integrity of the credit card system. We will continue to work with the industry in its efforts to resolve these problems. Necessarily, we must channel our limited investigative resources to the most productive use consistent with our law enforcement mission. We will become involved in credit card investigations when there is a violation concerning theft of the mail, especially if it appears that the theft occurred while the mail was in the custody of the U.S. Postal Service.

For us to become involved in an investigation of fraudulent applications for credit cards, there must be a large number of banks or issuers who have been victimized and a substantial financial loss.

And finally, with regard to violations of the Truth-in-Lending Act, we must closely analyze what relationship a particular violation has with our overall mission to protect the mails and the mail system.

It has certainly been our pleasure to report to you this morning the efforts of the Inspection Service to enforce Federal law with respect to credit card fraud. I will be happy to answer any questions you may have.

[Complete statement follows:]

Statement of Charles P. Nelson

Madam Chairman, I am Charles P. Nelson, Assistant Chief Postal Inspector for Criminal Investigations, thank you for the opportunity to appear before this subcommittee to discuss the efforts of the Postal Inspection Service to prevent and combat credit card fraud.

I would like to begin by telling you briefly about the Postal Inspection Service. The Postal Inspection Service is the investigative and audit arm of the United States Postal Service. We have investigative jurisdiction and enforcement responsibility over all violations of Federal law relating to the integrity and security of the mails, and the safety of all postal valuables, property and personnel. Our law enforcement investigations consist of two major categories: Criminal attacks upon the mails, postal facilities or postal employees, and those violations which involve the misuse of the postal system itself, such as mail fraud and misrepresentations or the mailing of bombs, narcotics or other nonmailable matter.

The magnitude of these responsibilities is in direct proportion to the size of the Postal Service itself which last year handled over 100 billion pieces of mail and has about 670,000 employers, over 39,000 postal facilities and cash income of about $23.3 billion.

With that introduction, let me move to the topic of credit card fraud.

The growth in the credit card industry in the late sixties led to a corresponding growth in credit card fraud along with an increase in our investigative activity in this area. In addition to responding to the industry problems through an aggressive investigative effort, we strongly urged and encouraged the creation and expansion of the security and investigative efforts within the industry. Equally important, during our national postal forums in Washington, D.C. in 1969 and again in 1970, we urged the industry to take action to protect itself and more importantly to stop contributing to the problem through such actions as indiscriminate mailings and inadequate verification of credit card applications.

As has been the case for fraud activity affecting other industries, the Mail Fraud Statute (title 18, United States Code, section 1341), until recently was the basis for most federal investigative activity in the credit card field. The Mail Fraud Statute is violated by devising or intending to devise a scheme to defraud which involves the use of the mails in furtherance of the scheme.

During the 1960s and 1970s, many successful prosecutions under the Mail Fraud Statute were obtained on the bais of two basic mispresentations: (1) That when the card was presented, the individual represented himself as the rightful owner of the card or that he was authorized to use it, and (2) that payment for the product, services, etc. obtained with the card would be made in accordance with the terms specified by the issuer of the card. The only use of the mails in many of these cases was on the mailing of the invoices back to the issuer of the card.

In addition, we obtained convictions under the Mail Fraud Statute where false information was furnished on applications. We also investigated and prosecuted many other cases where the credit card itself was stolen from the mails.

The highest volume of mail fraud cases involving credit card offenses was in 1972 when we investigated over 2,000 incidents of mail fraud relating to credit cards. These were usually relatively simple cases compared to the more complex ones we investigate today.

All this changed on January 8, 1974, when the United States Supreme Court, in a five to four decision, affirmed a Sixth Circuit Court of Appeals decision in *U.S.* v. *Maze* the court decided that mailings of credit card invoices between merchants providing services and credit card issuing agencies are not sufficiently related to a scheme to defraud to bring them within the purview of the Mail Fraud Statute, the court held that a scheme to defraud reaches fruition at the time the credit card is used and that the subsequent mailings of the invoices are not essential to or in furtherance of the scheme. Following this decision, the number of mail fraud credit card investigations decreased significantly.

Nevertheless, preventive actions taken by the industry along with the addition of the Truth-in-Lending Act of 1970 and other legislation has helped to fill in the gap left by the narrowing of the Mail Fraud Statute.

Section 1644 of the Truth-in-Lending Act makes it unlawful to utilize or transport in interstate commerce lost, stolen, counterfeit, fictitious, altered or fraudulently obtained credit cards with intent to defraud. The initial act required purchases totaling at least $5,000 on a credit card in one Federal judicial district in one year to constitute a violation. In 1974, Congress revised the statute so that it applies when $1,000 in fraudulent purchases are made in a Federal judicial district in a one year period.

Our investigations do not provide us any way of knowing how much credit card fraud there is in terms of dollars and cents. Such a figure can only be obtained from the industry itself. It should be remembered that by no means do we investigate all instances of credit card misuse. The Postal Inspection Servece is no more able to police the credit card system than it is to police the insurance or cents-off coupon industries or the numerous other business enterprises which depend on the use of the mails.

During fiscal year 1982, the Inspection Service completed 80 credit card fraud investigations and arrested 57 violators. There are a number of cases involving fraudulent credit card applications on the east coast where as many as twenty to thirty banks have been defrauded in amounts exceeding $100,000. To reduce this type of crime, we feel the industry still needs to improve its procedures for verifying applications to determine whether or not they are fictitious.

Let me give you a sampling of some of our more recent investigations.

In California, an international credit card fraud ring has defrauded several banks out of five to ten million dollars as a result of their activities. The gang unfortunately has members inside the Postal Service as well as the banking industry who are supplying credit cards to other gang members. The members then have merchants working in collusion with them who submit fraudulent vouchers to the banks imprinted with stolen credit card numbers. They run up charges to the credit limit and then move the cards out of the country. Even though the cards have already been run to their maximum financial limit, this does not prevent them from being used in foreign countries where the verification procedures are less stringent. Some of these individuals have been convicted and others indicted. Several are fugitives in foreign countries.

A series of investigations which began in New York City about four years ago has been of significant benefit to the credit card industry.

It all began with a family who operated a major preimprinted credit card scheme in the New York metropolitan area. The family distributed sales slips already imprinted through the use of lost or stolen credit cards to merchants who participated in the scheme. These merchants would then in turn send the fraudulent vouchers to the banks.

The involvement of 104 merchants was found through developing the fraudulent credit card history in connection with the cards seized at the family's residence. With these identifications, further investigation disclosed 750 additional stolen credit cards had passed through these stores.

Initially, three family members were arrested. Soon thereafter, the others fled the United States. Outstanding arrrest warrants are still in effect. Credit card losses attributed to this family are estimated at two million dollars. This investigation also led to the arrest and conviction of several of the individuals and merchants involved with the family.

Another investigation turned up what was commonly referred to as the "counterfeit white plastic scheme." The nine merchants involved in this scheme defrauded the industry out of $559,000. After information from legitimate cardholders and accounts was obtained, pieces of white plastic imprinted like a credit card were used on credit invoice slips. The slips were then sent through merchants working in collusion with the operators of the scheme to defraud the banks. Several of those involved have been convicted and sentenced.

A very recent investigation involved perhaps the most sophisticated covert operation against the credit card industry discovered to date. This involves the actual counterfeiting of credit cards. A silk screen painting process was developed in Los Angeles and then moved to the New York area. Several arrests and convictions have been obtained, while one of the people involved in this operation has been the victim of a gangland style murder. We have evidence that organized crime has been responsible for financing this counterfeiting operation. Recovered during this investigation was approximately $500,000 worth of equipment which was used to provide the fake credit cards. This activity has now moved into a stage where the counterfeiters are using an offset printing process to counterfeit the credit cards. Equipment utilized by these counterfeiters is identical to that used by the credit card industry itself. The quality of the cards is excellent and poses a severe threat to the entire bank card industry.

Law enforcement can only attempt to deal with some of the manifestations of the problem. It is not the solution. As we see it, a major problem now facing the bankcard industry is counterfeit cards and schemes using account information without cards. The industry itself must continue to identify and aggressively pursue the latest technological advances in security to ensure that the cards and the system are protected from fraud and abuse. Preventive measures to reduce or eliminate such activity are essential in order to preserve the integrity of the credit card system.

The credit card industry faces some tough questions:

1. What is it willing to accept as an operational expense in the way of financial losses?
2. What price is it willing to pay for security?
3. What value does it place on the integrity of the entire credit card system?

We will continue to work with the industry in its efforts to resolve these problems. Necessarily we must channel our limited investigative resources to the most productive use consistent with our law enforcement mission, we will become involved in credit card investigations were there is a violation concerning the theft of mail, especially if it appears the theft occurred from the custody of the Postal Service. For us to become involved in investigation of fraudulent applications for credit cards, there must be a large number of banks who have been victimized and a substantial financial loss. and finally, with regard to violations of the Truth in Lending Act we must closely analyze what relationship a particular violation has with our overall mission to protect the mails and the mail system.

Madam Chairman, it has been my pleasure to report to you the efforts of the Postal Inspection Service to enforce Federal laws regulating credit card fraud. I will be happy to answer any questions you may have.

Senator HAWKINS. Thank you, Mr. Nelson.

Senator D'Amato has joined us. Do you have a statement?

OPENING STATEMENT OF SENATOR D'AMATO

Senator D'AMATO. Let me commend you Madam Chairman for holding these hearings. The credit card fraud problem is one that is taking on monumental proportions and I think it is one which we should certainly focus our attention on.

Organized crime has also become involved in this area. It is an increasing concern. Just a few weeks ago I experienced a situation where somebody attempted to use my credit card number to rent a limousine. They just called up and ordered this limousine to be sent to a particular place. In many, many situations we find that goods and services are being obtained through the unauthorized use of an unsuspecting victim's credit card number. Once you've used that card at a restaurant, your number is up for grabs, so to speak. This is just one small aspect of a much bigger problem but it is becoming a real concern.

I, in turn, was forced to turn in the card for one with a new number.

It is evident that the statutes, do need some work. I think it is an area that we have to focus on and I commend our distinguished chairman for holding these hearings. I would ask to have my opening statement submitted for the record in its entirety.

I would first like to commend Senator Hawkins for having the foresight to confront this escalating problem of credit card fraud before it is allowed to grow to epidemic proportions. The credit card has become a major form of payment for goods and services purchased in this country and around the world.

In fact, the pervasiveness of credit card use in our society, from the well-known VISA and MasterCard to the smaller, private label bank cards, retail cards and gasoline cards, has transformed us from a cash society into one that relies heavily on credit. In recognizing this transformation, the integrity of the credit card payment system must be preserved.

Due to the multitude of credit card issuers with cards currently on the market, it is difficult to accurately assess the actual monetary impact credit card fraud has had on this country.

We can say with certainty, however, that losses run into the hundreds of millions, we also know that the ultimate loser as a result of this fraudulent activity is the consumer.

As a Representative of New York, the State that can unfortunately, but justifiably, be called the credit card fraud capital of the world, I have a special interest in this investigatory hearing.

Thus, I would like to thank Senator Hawkins for giving us the opportunity to shed some light on this issue by calling this hearing. Considering the expertise and experience she brings to the area of consumer fraud, I am certain this subcommittee will be able to directly confront and effectively deal with this issue. I look forward to working with Senator Hawkins toward this goal.

Senator HAWKINS. Thank you, Senator D'Amato.

Senator Dodd has joined us also. Do you have a statement?

Senator DODD. I don't have a statement, Madam Chairman, but let me again commend you for holding these hearings. I think it is worthwhile to get into this. I think it's a legitimate potential interest because of the possible connection with organized crime.

I have always been concerned as well with just the proliferation of credit cards and the marketing of them as well. This has been a good business for business and sometimes I think the effort to see to it that everybody in this country has at least one in their pocket has created some of the problem, quite frankly, and I would be interested to hear from our witnesses about that responsibility or that element of the problem. But I do commend you for holding the hearings and I think it's worthwhile.

Senator HAWKINS. Thank you, Senator Dodd.

It's interesting during the hearings this subcommittee held on the cost of consumer credit, the banks that testified that they made no money on the credit card operation. My question to them was why did they send them out, if, indeed, they made no money. It was interesting to read the exchange we had and that we're having in this hearing.

Senator DODD. Not only that, but we've had problems in the cash discount issue as a tangential problem for people who wanted to provide a greater discount to consumers if they used cash, and I think it was 5 percent—Senator Proxmire knows these issues intimately—the limitation on the amount of the discount that can be made available to consumers if they use cash.

Senator PROXMIRE. Five percent.

Senator HAWKINS. It's very common in Florida for credit cardholders for gasoline to have a sign outside that says 5 percent discount for cash.

Senator DODD. We're junkies, credit card junkies.

Senator HAWKINS. I believe in looking into this and making sure that those of us who are junkies are protected.

Chief Justice Berger dissented in the *Maze* case, Mr. Knapp, and characterized the Federal mail fraud statutes as a stopgap device to deal on a temporary basis with the new phenomena until particular legislation can be developed and passed to deal directly with the evil. That is the statement from Chief Justice Berger.

AMEND EXISTING STATUTES

Doesn't it follow that the Federal credit card fraud statutes should be strengthened so we'll not have to rely strictly on the mail fraud statutes?

Mr. KNAPP. I think the statutes can be strengthened in the way I suggested to you in my prepared statement, specifically broadening them to include counterfeiting and altering and also overcome some of these other defects in the way they have been interpreted.

Senator HAWKINS. A later witness will tell us about a foreign student group that's been operating on a nationwide basis a credit card fraud scheme to purchase merchandise in the United States to be shipped to their homeland before it's paid for. Do you know of any steps that are being taken by the Government to break up such operations like that?

Mr. KNAPP. I haven't heard about that specific transaction. That's probably one of the investigative agencies.

Senator HAWKINS. Well, a later witness will also tell us that U.S. attorneys are reluctant to use title XV and would prosecute more credit card fraud cases under title XVIII if it were amended to prohibit credit card fraud.

Mr. KNAPP. I don't think it makes any difference whether it's in title XV or XVIII. I think that rumor has gotten around, but whether it's XV or XVIII or XXXI or any other titles that we frequently use, it makes no difference. I think we can use the existing statutes and just amend them in the ways that I have suggested.

Senator HAWKINS. Do you have any evidence to show that judges and U.S. attorneys are beginning to take these crimes more seriously?

Mr. KNAPP. Yes. The problem has only magnified in the last year or two and it's really gotten out of hand in the last year or two as the statistics show and this is coming at the same time, of course, that we're trying to increase our efforts in narcotics prosecutions. We do have limited personnel resources, but the U.S. attorneys are becoming aware that this is a serious problem and we certainly will be giving it a great deal of attention.

WHITE-COLLAR CRIMES

Senator HAWKINS. Is part of the problem that the jails are crowded and maybe the judges don't really know what to do with these people since it is called white collar crime?

Mr. **Knapp**. I suspect there is a problem of jail crowding, both at the local and Federal level, and in close situations as to whether someone should go to prison or not, a judge is going to take that into consideration. So I certainly think something has to be done to expand prison facilities.

Senator **Hawkins**. I was interested in a case that was in my State lately where a dentist was convicted of some crime—I've forgotten what the crime was right now. The judge sentenced him to an extremely long number of hours giving free dental work which I thought was a unique way of paying back society that he had abused by giving good service to those people who the dentist had to serve without pay. It seems to me that unique sentencing like that is better than locking people up in a jail where it's too crowded anyway, and it seems to me that I'd be interested in any innovative sentencing that you're aware of in the Government's recommendations for sentencing like that.

Mr. **Knapp**. Well, innovative sentencing like that may be appropriate in the more local type crimes where small amount of credit card losses are involved.

Senator **Hawkins**. What's small in your mind?

Mr. **Knapp**. Well, I'm talking about someone who's not involved in organized activity. When you get into the organized activity where our priorities lie in terms of Federal prosecution, generally prison is the appropriate sentence.

Senator **Hawkins**. How successful have you been in prosecuting cases under the mail fraud statutes? What's your success rate?

Mr. **Foster**. Well, again in light of the *Maze* decision, we're not using the mail fraud statute generally. People from the Postal Inspection Service mentioned a while ago that we've been relying and we testified originally on the credit card statute to take the place of having to use the mail fraud statute. So there are a number of situations where we can still use the mail fraud statute in credit card situations, but they're very limited. We normally rely on the other.

Senator **Hawkins**. Thank you. Senator Proxmire was the next one in and I believe that's the rule we use on the Banking Committee. Senator Proxmire, do you have questions?

Senator **Proxmire**. Yes. Thank you very much, Madam Chairman, and I want to join the others in congratulating you on holding these hearings. I think they're very helpful.

ORGANIZED CREDIT CARD FRAUD

Mr. Knapp, you say in your testimony there's a substantial problem with organized crime activity but not the traditional organized crime. Then I noticed in Mr. Nelson's statement on page 6 he had a very interesting situation.

> In California, an international credit card fraud ring has defrauded several banks out of $5 to $10 million as a result of their activities. The gang, unfortunately, has members inside the Postal Service as well as the banking industry who are supplying credit cards to other gang members. The members then have merchants working in collusion with them who submit fraudulent vouchers to the banks imprinted with stolen credit card numbers.

So you've got the Postal Service involved, the banking industry, and the merchants all working together in this scam that's costing

$5 to $10 million. Wouldn't you call that kind of an organization? If that isn't organized crime, what is organized crime?

It's organized crime. When I use the term traditional organized crime, I'm referring to the Cosa Nostra type activities and things like that, what we traditionally view as——

Senator D'AMATO. You can get into trouble nowdays by tying the definition of organized crime to particular ethnic sterotype.

Senator PROXMIRE. Especially now because I don't know why this has to be identified with a particular——

Mr. KNAPP. I mean the so-called family type—but it is organized in the sense that we're getting into new kinds of organized crime.

Senator D'AMATO. When you refer to the organized crime you do not have to use that term. It does not reflect the reality of what actually constitutes organized crime in this country.

Mr. KNAPP. I'm sorry.

Senator D'AMATO. Obviously, you do not come from New York.

Senator PROXMIRE. At any rate, my question was related to who would have jurisdiction over these circumstances, the Postal Service or you, or would you both have jurisdiction in this California case that I cited? Perhaps Mr. Nelson can answer that.

Mr. NELSON. We accepted jurisdiction under that case and——

Senator PROXMIRE. Did you share it with the Justice Department?

Mr. NELSON. Yes; we reported it to the Justice Department and worked with them, and they pursued prosecution. It goes beyond that. Many of those credit cards when utilized to the limit, the limit the issuer sets, would subsequently be used in the Far East and Europe, and they'd continue to be used overseas because, I suppose, less stringent credit inquiries are required.

Senator PROXMIRE. So it was an international organized crime operation?

Mr. NELSON. It frequently becomes international.

Senator PROXMIRE. I notice, Mr. Knapp, in your statement something that I just think we ought to dwell on for a minute. You said the losses in 1981 and 1982 were nine times greater than for the past 7 years.

Mr. KNAPP. Yes.

Senator PROXMIRE. So if you figure that's only 2 years, 9 times greater than the past 7 years, that makes them on a per annum basis about 30 times greater. In other words, it's a real explosion?

Mr. KNAPP. Yes.

CREDIT CARD LOSSES EXCEED BANK ROBBERIES

Senator PROXMIRE. Furthermore, you also point out that the losses through credit card fraud are two and a half times greater than the losses through bank robberies. We're all concerned with bank robberies, but it's $128 million versus $46 million, so we're not just talking about peanuts here. We're talking about something that is very significant and serious and requires, it would seem to me, much greater attention, concern, and action than we've given it so far.

Now you have a fascinating example here on page 6. You say that credit cards may be obtained by the original card holder without an intent to defraud. They may later be sold or given to a defendant with the knowledge that the defendant would use the card to charge purchases without paying for them. Then the cards may be reported stolen or lost by the original card holder.

I imagine that that's one of the more common ways of defrauding; is that not the case?

Mr. **Knapp**. It's a fairly common way, yes.

Senator **Proxmire**. Yet when you give your recommendations at the end on page 8, I don't see any recommendation to cope with that particular way of stealing money.

Mr. **Knapp**. Yes; at the very last two lines where it says we will support amendments to expand the covered acts to obtaining or transferring cards as a part of a scheme to defraud. That was the intended cross-reference to the specific comment on page 6.

Senator **Proxmire**. Can you give us legislation that you recommend that we consider, draft it for us, and make it available to us so we can have your suggestions in legislative language?

Mr. **Knapp**. Yes.

Senator **Proxmire**. Mr. Nelson, how easy is it for Mom and Pop criminal firms to counterfeit a credit card?

Mr. **Nelson**. A Mom and Pop criminal firm, I would think, would have some difficulty counterfeiting a credit card. For organized groups it appears to be relatively easy.

Senator **Proxmire**. Why is it difficult for the——

Mr. **Nelson**. Well, the equipment that's needed.

Senator **Proxmire**. What equipment is needed?

Mr. **Nelson**. I can't explain, but the presses and the type of mechanization.

Senator **Proxmire**. How big an investment would it take to go into this business?

Mr. **Nelson**. Several hundred thousand dollars, I'd say, to get the proper equipment, and we've had groups that have had that much equipment. It's identical to the equipment used by the issuing bank.

Senator **Proxmire**. So it has to be a rich Mom and Pop.

Mr. **Nelson**. Very rich.

Senator **Proxmire**. What credit cards are the most difficult to counterfeit and which ones are the easiest?

Mr. **Nelson**. My understanding is the most difficult is the American Express, and we have only had one instance where they have been fairly successful—and that was in the Northeast—in reproducing American Express.

Senator **Proxmire**. Why is American Express more difficult?

Mr. **Nelson**. It has something to do with the coloring they use on the face of the card and the slants and the angles and the oblique ways of looking at it. MasterCard and VISA, for instance, are relatively easy to be counterfeited.

Senator **Proxmire**. How much would it cost for a card per year to make credit cards counterfeit-proof?

Mr. **Nelson** I can't answer that. I don't know.

Senator **Proxmire**. Apparently, American Express has come close to that.

Mr. **Nelson**. They have. That's true.

Senator **Proxmire**. And it's a very common card and you say that only one instance you know of it's been counterfeited?

Mr. **Nelson**. Only one that we are aware of. MasterCard, I believe, also has a new card that they're looking at that has a very unusual section in the center that when you turn it different ways it reflects different colors and is pretty much, from what the industry says, counterfeit-proof.

Senator **Proxmire**. For the record, could you make a study and give us a general notion of how much it would cost to make a credit card counterfeit-proof or virtually counterfeit-proof the way American Express has done it?

Mr. **Nelson**. Sure. We'll be happy to get together with some of the industry people and prepare something for you.

[Information subsequently supplied for the record follows:]

OFFICE OF THE CHIEF POSTAL INSPECTOR
Washington, DC 20260

July 14, 1983

Honorable William Proxmire
United States Senate
Washington, DC 20510

Dear Senator Proxmire:

Currently, MasterCard is the only company offering a secure and alleged counterfeit-proof credit card. The cost of production is an additional 2½¢ per card. The company began issuing these cards to new and present card holders March 31, 1983. MasterCard expects total distribution by 1986 when three-year cards sent out this year will expire and be replaced.

The Visa Credit Card Company is presently testing a new card that will contain a microchip. The marketing of this card is not expected in the near future because the estimated production cost of $5.00 per card is too great to be assumed by the consumer.

In a recent Credit Card Management Seminar conducted by the American Bankers Association, it was revealed the cost to produce secure cards ranged from .01 to $10.00 per card.

I have enclosed a copy of an article from the May 1983 edition of Security World Magazine which explains the security process employed by the MasterCard Company.

If I may be of further assistance, please contact me.

Sincerely,

C. P. Nelson

C. P. Nelson
Assistant Chief Inspector
Criminal Investigations

Enclosure

SECURITY TODAY

New Credit Card Deters Counterfeit

As credit card counterfeiting skyrockets among all major card companies, Mastercard recently introduced the first holographic credit card that is "difficult if not impossible to counterfeit."

Redesigned with three added security features, the new MasterCard credit card takes aim at a frightening trend. Losses attributed to credit card counterfeiting increased 340 times in five years at MasterCard, from $25,000 in 1977 to $8.5 million in 1982. Industry-wide losses rose 600 times, from $66,000 in 1977 to $40 million in 1982. According to a MasterCard spokesman, the method of reporting counterfeiting remained unchanged, which could account for the startling increase.

After six months of study, the new MasterCard charge plate was introduced March 31 and will be distributed to 75 percent of MasterCard holders within 18 months. The remaining 25 percent will be issued new cards before 1986, when three-year cards sent out this year will expire and be replaced.

The three new security features of the card are contained in the bottom horizontal 40 percent of the card representing the MasterCard logo. The upper 60 percent is reserved for the logo of the issuing bank.

- First, security is upgraded by fine-line printing on the lower one-half of the card. The word MasterCard is repeated over and over in faint lines that make silk screening, the most common method of counterfeit card production, more difficult.
- Second, ultraviolet ink on the MasterCard logo will make some of the printing fluoresce when passed under the ultraviolet light. This feature is intended for use by banks to check authenticity when a cardholder applies for a cash advance. Because most banks already have the necessary equipment they will not need to purchase new readers to utilize this security feature.
- Third, the most dramatic security change, a holographic metal foil strip on the vertical corner of the MasterCard logo will feature a globe and the block letters MC. Holograms are designs photographed with laser reference lights from two angles and then encased in one piece of plastic, thus appearing three dimensional.

Without holographic expertise and expensive equipment, counterfeiting of the design is impossible; and even with the capability, precise duplication is difficult. American Bank Note Company, a division of International Bank Corp., will supply the cards, and is the only firm with proper facilities to produce the holographic cards.

The new cards, which cost only 2½¢ more to produce than the current card, will maintain the current numbering method in which the la number is an algorithm of the oth numbers. When cards are tampere with and numbers are changed, authorization is given to cards wi final numbers that do not correspond to the algorithm. Also, some of the final digits in the new cards will overlap with the hologram so that changing card numbers demands reproduction of the hologram.

"We are certain to discourage counterfeiting of MasterCards," a spokesman said. "And other companies are likely to follow suit because their cards will become more vulnerable as ours becomes more difficult to reproduce."

MasterCard has announced three new design features that will help it reduc counterfeiting of its card. The most unique approach involves the use of holograms, which are virtually impossible to reproduce exactly.

Senator **Proxmire**. Is there an active market for valid credit card numbers?

Mr. **Nelson**. Yes.

Senator **Proxmire**. Counterfeit cards?

Mr. **Nelson**. Yes.

Senator **Proxmire**. How does that market operate?

OPERATION OF COUNTERFEIT CARDS

Mr. **Nelson**. Well, it operates in many different ways. Perhaps I could describe a couple of investigations and give you some idea.

There was one group, again quite well organized in the Northeast, that would obtain the information when you went in and made a purchase. They had your number and the expiration date of your card, and they would turn around and use what the industry and law enforcement refer to as white plastic. It's a plastic similar to the size of your credit card. They emboss it with the numbers that appeared on your card. They just look at your invoice and prepare it and do that with hundreds of cards and have boxes of invoices and preprint them. In this one investigation I think we had over 100 merchants who accepted these preprinted invoices.

Senator **Proxmire**. What does it cost to buy one of these cards?

Mr. **Nelson**. About $50 or $60, I'd say. At any rate, they would use the invoices and print them up and submit them to the bank just as if they had made sales at their establishments when in fact they had not.

Senator **Proxmire**. Thank you.

Senator **Hawkins**. Senator D'Amato.

Senator **D'Amato**. By the way Mr. Knapp, I am sure you understand why I made that reference to organized crime and the tendency to stereotype certain ethnic groups.

Mr. **Knapp**. No; what I meant——

Senator **D'Amato**. And I take exception to that and my Mother would take exception and my grandparents would take exception. So I think we have to be very careful about that. I too would like to see that those elements in our society are dismantled. That we do everything possible to reach this goal. But I think we greatly minimize the problem when we associate, whether intentionally or not, organized crime with one particular ethnic group. By the way, I finally qualified for a gold card. This is the one they tried to charge the limousine on. They obviously got the number from a restaurant and just called up and gave it to the limousine service. To an extent, credit card systems invite this activity as part of a marketing scheme. They advertise on television today that if you want a new telephone you can buy the telephone by just calling and giving your credit card number over the telephone.

There is also a real problem now in producing fraudulent credit cards. I will give you some of the statistics. Overall fraud losses for VISA and MasterCard were at $125 million for 1982. Does that square with your numbers?

Mr. **Nelson**. I don't have those figures.

Senator **D'Amato**. OK, let me give them to you. New York is the most active area in the country for credit card frauds. Florida is a close No. 2. Overall fraud losses for VISA and MasterCard were estimated at $125 million for 1982. That was up 1,000 percent or 10 times 1972 losses. In comparison to bank robberies—I think Senator Proxmire mentioned this—in 1982 you had bank robberies that totaled $46.8 million. So in just VISA and MasterCard alone it was $125 million—in losses—a significant problem.

I mention that because it appears that the main thrust of the two statutes in question, the truth in lending statute and the electronic funds transfer statute does not address this serious problem and it is a growing problem in this country. We are going to wake up some day soon and we will have a problem of major proportions. I know that VISA and MasterCard have suggested legislation that would very comprehensively deal with this problem. I think the court case where certain defendants almost escaped conviction because they did not actually use a card, but used, instead an identification number, points up a glaring deficiency in the law.

That being the case, what type of revision to the current law would you recommend to rectify this situation and would you support the legislative recommendations made by the VISA Corp., which would involve a two-pronged adjustment, both revising the existing law and adding to the Federal criminal code a new chapter that comprehensively addresses this kind of innovative criminal activity?

Mr. KNAPP. I haven't seen the latest VISA proposal in terms of all the specifics. We do not believe in general that a comprehensive revision is necessary.

Senator D'AMATO. You do not think the States can attack with this alone, do you?

Mr. KNAPP. No. What I'm saying, as I indicated in my prepared statement, there are amendments to the two existing statutes which could be made, which would adequately strengthen our prosecutions without going through the necessity of reenacting a totally new chapter or statute.

Mr. NELSON. I'm not that conversant with the suggested changes.

Senator D'AMATO. Are you conversant with them, Mr. Nelson?

Mr. NELSON. No, I'm not, but we have had no difficulty in our cases in getting the prosecutions under S. 1644 and S. 1341. We have not detected any real problems in that area.

Senator D'AMATO. Well, you certainly have the one problem with respect not being able to prosecute the people who use just the numbers without the cards, right?

Now let me ask you something. This little card is becoming more and more pervasive and I do not argue against their use if people want to use them. If you give somebody cash nowadays it is incredible. Sometimes they do not know what to do with it. Hardly anybody carries money.

Am I correct in saying that you have detected a growing trend in the counterfeiting of these cards?

Mr. NELSON. Yes; I'd say we have. In that one incident I talked about, along with one of the arrests in that case, we recovered 7,000 counterfeit cards like you have in your hand. It's the first time to our knowledge that the American Express card has been counterfeited and it is growing. It's national. We've had it in New York, and we have it on the West Coast and we've had it in the South.

Senator D'AMATO. This is currency?

Mr. NELSON. Absolutely.

CRIMINAL PENALTIES NOT STIFF ENOUGH

Senator D'AMATO. And so why not a comprehensive revision of laws relating to the counterfeiting of these cards so that we would prosecute and punish those who counterfeit these cards with the same vigor as we would those who counterfeit U.S. legal tender. I think we should really begin to examine the current statutes in light of the analogy to be drawn between credit cards and currency. If we are going to stop this kind of thing, I think we will have to step up enforcement by tightening criminal liability provisions and the penalties that flow therefrom to something beyond a slap on the wrist. For those who would either counterfeit or would pass counterfeit money, we provide pretty tough penalties, because we are guarding our Nation's money system. The integrity of that is absolutely imperative to the free flow of commerce, is it not?

Mr. NELSON. Yes; I agree with your proposal. My remark that we have had no problems was not to say that the law does not have to be looked at or not adjusted, but we have experienced no prosecution difficulties with the two statutes that we're presently working under.

Senator D'AMATO. Mr. Knapp, I think you feel that the present laws are adequate, that the penalties are severe enough, because we tend to think of this possibly as isolated instances of minor criminal activity: fraudulently someone purchases $100 worth or $200 worth of clothing, et cetera, or buys one of these cards for $50. But it seems to me that this kind of repeated situation undermines and creates tremendous problems, not just for VISA and Mastercard, but for the integrity of our credit payment system; and thus should not treat those who would counterfeit forge credit cards, in the same manner with which we deal with those who would forge our legal tender.

Mr. KNAPP. Excuse me. May I have a second? The maximum existing penalties provided under the statutes now is 10 years. The question is what penalties are going to in fact be enforced. I think the statutes provide sufficient penalties. The statutes need to be broadened in the ways I indicated and the judges have to realize in sentencing people that they should be giving them basically time in prison as a general rule when there's any substantial amount of activity involved. So it's a question of using the existing statutes in terms of penalties in a more forceful and effective way.

Senator D'AMATO. Should they have mandatory minimums?

Mr. KNAPP. In the administration so far we have tended to shy away from mandatory minimums except in a limited number of areas, and those are set forth in the President's crime bill. The mandatory minimums are in effect pretty new to the Federal System right now and we are somewhat cautious in using them because it really does destroy all flexibility on the part of the sentencing judges. I think the general presumption should be that crimes of this sort where there's any significant amount of loss involved should receive some form of incarceration.

Senator D'AMATO. All right. My time has expired I will for the record submit to you questions dealing in detail with the proposed legislation put before us as suggested by VISA and Mastercard to deal with this and I'm asking you if you would not please respond to them.

Mr. KNAPP. Yes; we'll respond specifically to specific provisions.

Senator D'AMATO. In those areas where you think there are deficiencies in current law, I would also ask you to come forth with legislative proposals to deal with those problems that you and Mr. Nelson have attested to rather than this committee going forward with their own proposals without the Department of Justice's support.

Mr. KNAPP. Yes.

Senator D'AMATO. I thank you.

Senator HAWKINS. Senator Dodd.

Senator DODD. Thank you, Madam Chairman.

Let me move first of all, Mr. Knapp, that one of the problems you cited in your testimony this morning is a problem that's been identified by one or more of the credit card companies having to do with the basic Federal law regarding what triggers Federal jurisdiction, being the $1,000 minimum amount of money involved, and the distinction that exists between a scam or a scheme and where a number of credit cards may be involved and very cleverly never exceeding the theft of more than $1,000 per credit card.

So, in effect, you can avoid the federal jurisdiction in that regard. You cited the problem but you didn't take a position in here on that. What do you think ought to be done? Do you understand what I'm talking about?

Mr. KNAPP. Yes; I think so. Existing law has a provision for aggregating sums so you can get over that $1,000 threshold. I don't know how they phrase their specific suggestion and I'll take a look at it, but ——

Senator DODD. Apparently they lost a case on that issue in the courts, that they've been told in effect that the scheme or the scam doesn't apply. I think it's VISA that's made the suggestion to modify the law and you cite the problem in your testimony. You just didn't take a position on it. Do you think we ought to modify the law in that regard?

Let me just cite for you the statistics. The types of problems with fraud, lost credit cards amounts to 29.2 percent. This is VISA International, 29.2 percent are lost. The average dollar amount is $1,047, right on the border. Stolen credit cards amounts to 35 percent of VISA's problems. The average dollar amount in stolen credit cards is $650. The credit cards not received, the mail problem, about 18.7 percent of their problems, and that's $1,519. Counterfeit is 11 percent of VISA's problems and that average dollar amount is $1,102. Interesting, lost and stolen, which would become more of a consumer problem, they're just not watching their card or someone loses it, that's almost 65 percent, but the dollar amount is $650. You're stuck on 35 percent of the problems, you can't get in. If someone is stealing a bunch of credit cards and only using one credit card to buy $650 worth of merchandise, at least one court said you can't get them under Federal jurisdiction. Why not change the law, if in fact there is a scheme and if in fact the courts have had difficulty with that already?

Mr. KNAPP. Well, S. 1644 presently is phrased as follows: "Use or attempt or conspires to use any" et cetera "to obtain money, goods, services or anything else of value which within any 1 year period is a value aggregating $1,000 or more. That language is pretty broad.

Senator DODD. I don't know if we have the citation.

Mr. KNAPP. I would have to look at the specific case, but we would be certainly glad to consider plugging any loopholes.

Senator DODD. I wish you would. Do we have the case number? Well, we'll get it for you.

Mr. NELSON. There have been court decisions both ways on that. There have been decisions where the court said one credit card, $1,000, and there have been decisions, as he was alluding to, that say you can aggregate it.

Senator DODD. I was not aware of the other court cases, but obviously there's some confusion.

INVESTIGATION AND PROSECUTION HAS NOT BEEN EXTENSIVE

The other point is in your responding to Senator Proxmire on the organized crime question and how much of this is what we traditionally think of as organized crime, and I understand your distinction speaking specifically of organized crime in this country and all that that involves, and you draw some pretty—you describe the problem. It's significant and massive and the numbers indicate that. And yet the Federal investigation and prosecution effort, according to your testimony, has not been extensive.

Postal inspection service has investigated 80 credit card frauds in 1982, EFT, 9, since October 1, 1982; 89 cases. You haven't by your own admission done an extensive investigation and prosecution and yet you draw some pretty emphatic conclusions. How do you explain that?

Mr. KNAPP. Well, as I indicated, this is a problem which has just mushroomed in the last year or two and it's unfortunately occurred at a time when other crime problems were mushrooming too. As I said, I think in the coming years you're probably going to see a greater amount of Federal prosecutions for this type of crime.

Senator DODD. What are you doing right now? These statistics run up to when?

Mr. KNAPP. March, in terms of prosecutions that have actually been initiated. I think Mr. Nelson can better speak for the Postal Service.

Mr. NELSON. We have confined our activities basically to the organized groups, and in fiscal year 1982 we closed 80 cases, and we had indicted something like 47 or 48 people, but they're very well organized. In one case we had witnesses in protective custody, and a man and wife and their 6-year old son were just gunned down gangland style.

Senator D'AMATO. Where was that?

Mr. NELSON. New York.

Senator DODD. Where the limousine was rented?

Senator D'AMATO. You couldn't say Connecticut?

Senator DODD. We send them all to New York. [Laughter.]

Mr. Nelson. Another case involved the silk screening method of counterfeiting credit cards. There had been an arrest of one of the two prime movers of the whole scheme, and it involved millions of dollars, and his associates became worried about him, and he ended up with 10 bullets in his head and stuffed in the trunk of a rented car.

Senator D'Amato. I'm not going to ask where that was.

Mr. Nelson. It is a well-organized effort, and you talked about students—we had a group of Nigerians and another group that called itself the Black Hebrews that made purchases all over the country and shipped the merchandise out.

Senator Dodd. Now that you know all this and you reached the conclusion it's an explosion, what sort of resource allocation has there been either within the Department of Justice or the Postal Service to deal with the problem? You're obviously aware of it. What are you doing?

Mr. Nelson. We are dealing with what I refer to as the organized groups. We are not dealing with, well, let's say, a credit card case where a false application is submitted and someone runs up $500 on that credit card. We simply cannot approach all those. We don't have the resources to do it, and I agree with Mr. Knapp in that respect, I think that's a local problem. The local law enforcement and the State law enforcement can handle that.

Last year I think we devoted 19,000 investigative hours to credit card type frauds.

Senator Dodd. 19,000?

Mr. Nelson. Yes.

Senator Dodd. Is that a lot by comparison to what you did in other areas? It sounds like a pretty high figure.

Mr. Nelson. I think it's adequate for the problem we have. It's maybe a little higher. In the one case I mentioned earlier, we had two inspectors working undercover for 4 years and teams to back them up. We put a lot of effort into these big cases.

Senator Dodd. In this VISA figure of cards not received which they identify as being about 18 percent of their problem, I presume undercover within your service that was to identify employees who were involved in stealing?

Mr. Nelson. That is right, and those hours are not included in the hours I just mentioned. We refer to that program as internal crimes. Fraud is external, basically involving non-postal people.

Senator Dodd. Is it basically non-postal?

Mr. Nelson. Yes.

Senator Dodd. The cards not received?

Mr. Nelson. The cards not received?

Senator Dodd. Yes.

Mr. Nelson. They are basically, probably, postal people, clerks and carriers.

Senator Dodd. That's my question. What have you found out?

Mr. Nelson. I can't tell you the number of hours devoted to that. Internal crimes involve about 30 to 35 percent of our total criminal resources. I'm not really sure of the hours. I can let you know.

Senator Dodd. VISA identified that as 20 percent of their problem is in that area. You're telling us that that's basically a postal employee problem.

Mr. **Nelson**. To the extent the cards get into the mails. It's also a bank problem. A lot of bank employees are identified removing sacks of cards or trays of cards before they ever get to the Postal Service.

Senator **Dodd**. Thank you.

Senator **Proxmire**. Would the Senator from Connecticut yield?

Senator **Dodd**. Certainly.

Senator **Proxmire**. Mr. Knapp pointed out before you came in—he didn't have it in his prepared statement—he pointed out that there was only one Federal prosecution using credit card statutes and none using the EFT statutes.

Mr. **Knapp**. No; one now using the EFT statute, but it's a substantial or a fair number using the Truth-in-Lending statute. Unfortunately, we don't have statistics to break down exactly how many are credit card and how many are other prosecutions under that section, but under S. 1644, I'll just give you an indication that the average we had about 25 in 1982, 27 in 1981, 9 so far this year. Unfortunately, I can't say that they're all credit card.

Senator **Proxmire**. Just one other question. Mr. Nelson, I understand there's a store in Times Square that sells credit card numbers, is that right?

Mr. **Nelson**. That's not outside the realm of possibility. I have no direct knowledge of it, however.

Senator **Dodd**. I just tried to do some quick math. You said 19,000 hours last year. Well, one employee working a 40 hour week, 50 weeks is 2,000 hours. When you give us this 19,000, you're talking about 7 or 8 people.

Mr. **Nelson**. Well, you have to consider vacations, sick leave and other things.

Senator **Dodd**. I did. Ten people.

Mr. **Nelson**. Yes, 10 or 11 people full-time.

Senator **Dodd**. Do you think that's adequate given the magnitude?

Mr. **Nelson**. We have addressed the major problems that we are aware of. We certainly have.

Senator **Dodd**. Do you think that's adequate enough people to be working on this problem?

Mr. **Nelson**. At this time, I do.

Senator **Dodd**. How many people do you have working on it, Mr. Knapp?

Mr. **Knapp**. That's the problem. We have our fraud section in the Criminal Division which deals with this and other issues of fraud, but most of the Federal prosecutions would be handled in the different U.S. attorneys' offices and it's just hard to break it down in terms of numbers of people devoted to this problem.

Mr. **Nelson**. There's one other thing you should consider in those hours. In all these cases, especially the lengthy undercover cases, we have personnel from sheriff departments and police departments who are assigned to us full-time. I think we had four New York detectives on one of the large cases up there who basically worked for us for several years.

Senator **Dodd**. Thank you.

Senator **Hawkins**. Thank you. I'll dismiss the panel at this time.

Our second panel consists of Mr. John Alexander, senior vice president, Bank One of Columbus, Ohio; Mr. James R. Branam, Jr., senior vice president, Southeast Services, Inc., Miami, Fla.; Mr. William Neumann, vice president for security, VISA International; and Mr. Thomas Kelleher, vice president for Security, MasterCard International.

In the interest of time we'd ask that you summarize your statement and submit your entire statement for the record and we will call first upon Mr. Alexander.

STATEMENT OF JOHN G. ALEXANDER, SENIOR VICE PRESIDENT, BANK ONE OF COLUMBUS, COLUMBUS, OHIO, CHAIRMAN, AMERICAN BANKERS ASSOCIATION, TASK FORCE ON CREDIT CARD FRAUD

[Complete statement follows:]

Statement of the American Bankers Association

Madame Chairman and members of the Subcommittee, my name is John G. Alexander, Senior Vice President, Bank One of Columbus in Columbus, Ohio. I am representing the American Bankers Association in my capacity as Chairman of the Association's Task Force on Bank Card Fraud.

The Association membership consists of over 90 percent of the approximately 14,500 full service banks in this country. The combined assets of nearly 13,000 members banks represents approximately 95 percent of the industry total. Approximately 90 percent of our members can be described as community banks having assets of $100 million or less.

Our Association welcomes the opportunity to present our comments on the problems associated with card fraud. We have become increasingly concerned with this issue. Ten years ago fraud losses in the bank card industry were not sufficient to cause great concern. However, in the last few years losses have grown at a geometric rate. Attached as Appendix A to this statement is a graph showing the combined losses of the VISA and MasterCard systems over the past ten years. The losses have grown from a combined $11.7 million in 1972 to $125.8 million in 1982—over a 1,000 percent increase.

We are particularly concerned about the counterfeit and altered card losses. For the MasterCard and VISA systems, these losses have increased from a relatively minor $175,000 in 1978 to over $20,000,000 in 1982). When these losses are aggregated with the losses involved in private label bank cards, retail cards, gasoline cards, and travel and entertainment cards, it is clear that the country is faced with major criminal activity that cannot be ignored.

INDUSTRY EFFORTS

In February of 1982, the Bank Card Division of the Association formed the Task Force which I chair, in an attempt to develop a comprehensive analysis of the growing counterfeit and alteration problems. Working closely with VISA and MasterCard, we have developed an effective industry program to focus on this problem.

The Task Force has recommended a number of changes to the two card association. These changes have been implemented or are being implemented by the associations in a timely and thoughtful manner. Senior management and governing boards have made major commitments to address the issue on a long term basis. Security personnel at both associations have been notably increased. Both associations have committed to incorporate new card secure properties to deter counterfeiting. New systems such as cancelled or fraudulent merchant indexes and counterfeit reporting systems are being implemented. New policies on card manufacturing, card embossing, and card transportation services have been or are being implemented. Rewards for the recovery of altered or counterfeit cards at point of sale have been implemented or increased. Portions of VISA's card recovery bulletin and MasterCard's restricted card list are being used to educate merchants on this problem. Communication and education efforts have been initiated with banks, enforcement agencies, and merchants and between the two associations.

The Task Force is developing a Card Fraud Manual. This manual is designed for banks as a manger's guide for developing a comprehensive fraud prevention and control program. The manual will provide guidelines for dealing with card manufacturers, guidelines for protecting account information, procedures and policies for staff training, procedures for merchant training, educational material for the consumer, and other useful guidelines for comprehensive fraud prevention.

On June 10, 1983, ABA will sponsor the first national Card Fraud Management Seminar. This seminar will be teleconferenced to five cities: New York, Atlanta, Dallas, Chicago, and San Francisco. This program will subsequently be available for state banking associations and other groups interested in sponsoring fraud seminars.

Finally, together with MasterCard and VISA, the ABA Task Force is sponsoring a major study of cards secure properties. Card secure properties are the physical aspects of the card that make counterfeiting or alteration more difficult. This study, undertaken in the fall of 1982 by Battelle Laboratories of Columbus, researched other industries for applicable technology that could be utilized in the card industry. To date, over 100 technologies have been tested. Some technologies were recommended for immediate implementation. Other promising technologies have been singled out for further study.

This effort has already resulted in many changes to be implemented by the VISA and MasterCard systems. MasterCard, for example, has announced plans to have all cards issued in that system include holograms, fine line printing and ultra violet inks. VISA is undertaking a comprehensive review of the technologies involved in the Battelle study with a commitment to incorporate the best in the new VISA card.

NEED FOR LEGISLATION

These efforts of the industry should help to substantially reduce the current fraud activities. However, in spite of the industry's best effort, we must understand that the criminal element is always just one step behind the new technology of the industry. As our methods for detecting and eliminating fraud become more sophisticated, so do the criminal activities designed to beat the system. Effective law enforcement is the only way to ultimately deter criminal activity.

As a result, the industry has determined to pursue a major revision of the law in this area which would include the addition of a new Chapter to the Criminal Code (Title 18, U.S.C.). This effort to modernize the law and focus attention on this growing problem would provide investigators and prosecutors with a clear and direct statute aimed specifically at card fraud. We view this major revision as part of the comprehensive law enforcement efforts necessary to deal with this problem on a long term basis. We are and will be discussing these proposals with the Judiciary Committees in both the Senate and House.

At the same time, we feel that minor amendments to the Truth-in-Lending law and the Electronic Funds Transfer Act are needed to fill some obvious and immediate gaps in current federal legislation.

In recent years the emphasis in criminal activity has shifted away from taking advantage of isolated lost and stolen cards to the more organized criminal activities involving alteration and counterfeiting of cards. Unlike fraud committed with the use of lost or stolen cards, the schemes involving counterfeit or altered cards rely heavily on the use of valid account numbers. As a result, the trafficking in account numbers has increased dramatically. For example, account numbers are used in collusive merchant's schemes where valid account numbers are embossed on white plastic and used to imprint sales slips.

In spite of this and other counterfeiting schemes using primarily account numbers and not cards themselves as the means for fraudulent activity, the Truth-in-Lending law is not clear that misuse of these account numbers constitute credit card fraud. At least one court has held that fradulent use of an account number did not constitute the illegal use of a "credit card".

An additional enforcement problem has been raised in connection with the $1,000 limit contained in several of the subsections of Section 134 of the Truth-in-Lending law and Section 916 of the Electronic Funds Transfer Act. Those subsections require that a minimum of $1,000 in money, goods or services be obtained within a one year period to create a crime punishable under the federal law. Case law is not yet clear whether these subsections require that the prosecutor show only that $1,000 in value has been obtained using card fraud or whether the prosecutor must show that $1,000 was obtained with a particular counterfeit, lost, or stolen card.

We urge this Subcommittee act to cure these defects before law enforcement efforts are further hampered. The industry has supplied language to the Subcommittee which we feel appropriately addresses the problems. (See Appendix B)

SAFEGUARDING THE ACCOUNT NUMBER

As fraud activity has increased, the industry has become increasingly aware of its responsibility to safeguard the account numbers of its customers. Efforts to protect account information is a major part of the efforts of the ABA Task Force. Our upcoming seminars and manual on fraud will provide banks with significant new information on policies, procedures, and technologies that will protect account information from falling into the hands of those who might use it illegally.

Our efforts will strive to educate banks, merchants, service agents, and customers on how to protect this information. Since card issuers are the primary victims of the fraud schemes, the efforts must begin with the card issuer.

Simple procedures now being suggested for all participants in the system which will help to eliminate much of the problem. For example, banks and processors can restrict access to account information or use only that portion of an account number necessary to identify the account in in-house activities. Merchants can utilize perforated carbons, carbonless sales slips and otherwise take precautions in disposing of carbons and duplicate sales slips. Credit bureaus or other service agencies can use only a portion of the account number where possible. Consumers can be educated to safeguard account numbers and sales receipts. Unless the information is safeguarded by each participant, the system is vulnerable to penetration by the criminal element.

As mindful as we are of our responsibilities in this area, we cannot support legislation which unduly restricts the bank's ability to disclose account numbers to third parties.

We must express our grave concern over the approach utilized in Section 2 of H.R. 2885 recently introduced in the House. That bill contains a broad proscription against the disclosure of account numbers and then provides only limited exceptions to the proscription.

The industry believes this is the wrong approach for two reasons. First, the industry has a strong interest in protecting account numbers. A proscription against disclosure will not significantly enhance that interest. This self interest should not be discounted as an effective means for insuring that the industry will quickly address conditions that allow account numbers to fall into the wrong hands. Without a quick response to such conditions, the industry is certain to experience increased losses. The consumer's liability for fraud loss is limited to $50 under Truth-in-Lending and the card issuing institution generally must bear the rest of the loss. In addition, a less than comprehensive response to a breach of security will lead to a decrease in the customer base for the institution. Without a strong customer base, a card operation cannot be profitable.

Second, this approach will add a compliance burden to bank operations that is unnecessary. As new rules are devised by the Federal Reserve Board, each legitimate disclosure on an account number would have to be scrutinized to be sure it fell within one of the limited exceptions. Where it did not or the application of the rule was unclear, the bank would be forced to petition the rulemaking body for an interpretation or an amendment. In effect, the time and resources of the banks and the taxpayers would be directed at meeting the compliance and regulatory burden and not at stopping those who intend to defraud the banks and the consumers.

If a general proscription is used, the exceptions must be broad enough to cover all legitimate uses of account information. We have identified nine general areas where account information must be disclosed. A description of these areas will highlight the difficulty in drafting legislation with exceptions broad enough to avoid problems in rulemaking, compliance, and interpretation.

Authorization systems.—In protecting cardholders, merchants and card issuers use extensive card authorization systems. Protection of consumers necessitate disclosure of account information including account numbers among the various parties involved in the systems. Account information will be disclosed to merchants; banks acting as merchant banks for retailers; independent authorization services acting as agents for merchant banks or issuing banks; and the VISA or MasterCard system.

Processing.—The same parties involved in the authorization systems are also involved in the processing of sales slips between banks, the processing of bank card statements for consumers and the collection and settlement of accounts between consumers and banks and between banks.

Collection activity.—Disclosure of account information to third parties is necessary in effort to collect delinquent accounts.

Credit bureaus and other creditors.—Banks typically disclose account information to credit bureaus and receive account information from these bureaus. The exchange of at least part of the account number is necessary to insure that the person or account is correctly identified. In addition, creditors sometimes directly exchange account information including account numbers as part of the process of verifying credit applications and in protecting against fraudulent activities. Check authorization systems may utilize account information.

Government agencies.—Disclosures of account information to government agencies is frequently required or desirable. First, bank examining agencies, both federal and state, are routinely given access to account information as they review the safety and soundness of a financial institution or check for compliance with consumer regulations. Second, disclosures are made to federal agencies under the Right to Financial Privacy Act and to state and local governments under similar state requirements. Finally, banks may desire to voluntarily provide information to law enforcement agencies where the bank fears either an attempted fraud on the bank or other illegal activities in connection with an account.

Sale of bank or card portfolio.—Banks often disclose account information to potential purchasers of a bank or bank stock or potential purchasers of all or part of a credit card portfolio. Potential purchasers desire to examine records for accuracy and to verify compliance with federal and state laws.

Court disclosures.—Banks are often requested or required to provide account information to parties involved in private litigation involving an account holder, i.e., divorce proceedings. In addition, on some occasion a bank may need to voluntarily disclose account information to a court in order to protect the interest of the bank. An example of this would be the filing of a proof of claim in a bankruptcy proceeding.

Marketing efforts.—Banks may disclose account information to related companies such as another subsidiary of the bank holding company in order to provide the cardholder with an opportunity to purchase new products or services. Account information (but not account numbers) may also be provided to third parties offering particular products or services deemed beneficial to the cardholder.

Other legitimate business purposes.—Account information is often disclosed in connection with other legitimate business activities of a financial institution. Information may be disclosed to a certified public accountant in an audit of the institution's financial statement. A lawyer may be given access to information in connection with litigation on behalf of or against the bank.

These examples indicate the complexity involved in specifying with completeness and accuracy all of the legitimate reasons for transfers of account information.

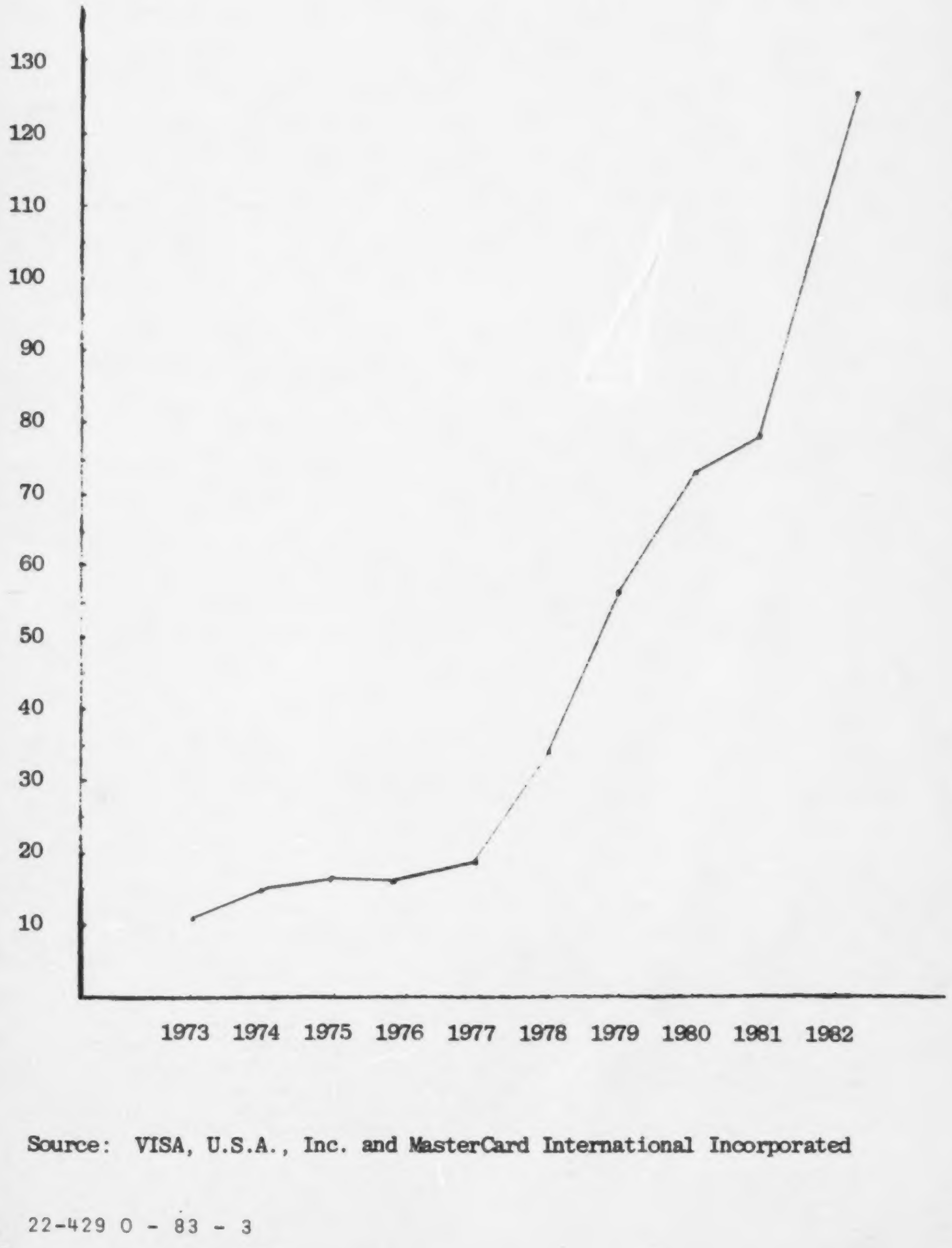
For these reasons, we cannot support legislation directed at financial institutions or others who are already working to protect account information. Legislation, if it is necessary, should be directed at those who transfer the information with the intent to defraud or for purposes other than legitimate business purposes. Attached as Appendix B is language suggested by the industry as the proper approach in this area.

CONCLUSION

We commend the Subcommittee for its attention to this serious and growing problem. We appreciate the opportunity to make our views on this matter known. We will commit our time and resources to assist the Subcommittee in fashioning and implementing a proper legislative response.

Appendix A

CREDIT CARD INDUSTRY
TOTAL FRAUD LOSSES
($ Million)



Source: VISA, U.S.A., Inc. and MasterCard International Incorporated

APPENDIX B.—DRAFT OF MAY 5, 1983, TITLE 15

[A BILL TO AMEND THE TRUTH-IN-LENDING ACT AND THE ELECTRONIC FUND TRANSFER ACT]

SECTION 1. The Truth-in-Lending Act (15 U.S.C. §§ 1601 et seq.) is amended by adding a new section to be designated section 129 to read as follows:

"Sec. 129. No person in a transaction affecting interstate or foreign commerce, or using any instrumentality of interstate or foreign commerce, shall buy, sell, furnish, exchange, obtain, transfer, deliver, or receive one or more credit card account numbers in any form—

"(a) with the intent to defraud any consumer or other person; or

"(b) for any purpose other than legitimate business purpose involving the credit card account or accounts, the cardholders, or the operation of the credit card system."

SEC. 2. Section 134 of the Truth-in-Lending Act (15 U.S.C. § 1644) is amended by redesignating the existing section as paragraph (a), by redesignating existing paragraphs (a), (b), (c), (d), (e) and (f) as paragraphs (1), (2), (3), (4), (5) and (6) and by adding a new paragraph (b) to read as follows:

"(b) As used in this section, the term "credit card" means a card, plate, coupon book, code, actual or fictitious account number, or other means of access, which if used alone or in conjunction with another credit card would permit a person to obtain credit or initiate an extension of credit. The aggregate one-year dollar values used in this section are to be calculated on the basis of the person or persons engaging in one or more transactions using one or more credit cards."

SEC. 3. The Electronic Fund Transfer Act (15 U.S.C. §§ 1693 et seq.) is amended by adding a new section to be designated section 922 to read as follows:

"Sec. 922. No person in a transaction affecting interstate or foreign commerce, or using any instrumentality of interstate or foreign commerce, shall sell, buy, furnish, exchange, obtain, transfer, deliver, or receive one or more account numbers in any form—

"(a) with the intent to defraud any consumer or other person; or

"(b) for any purpose other than a legitimate business purpose involving the account or accounts, the account holders, or the operation of the debit account system."

SEC. 4. Section 916(c) of the Electronic Fund Transfer Act (15 U.S.C. § 1693n(c)) is amended to read as follows:

"(c) as used in this section, the term "debit instrument" means a card, plate, code, actual or fictitious account number, or other means of access (other than a check, draft, or similar paper instrument) which if used alone or in conjunction with another debit instrument would permit a person to initiate an electronic fund transfer, whether or not the account accessed by the transfer was established primarily for personal, family or household purposes. The aggregate one-year dollar values used in this section are to be calculated on the basis of the person or persons engaging in one or more transactions using one or more debit instruments."

SECTION-BY-SECTION ANALYSIS

The proposed legislation makes two changes to the Truth-in-Lending Act and two analogous changes to the Electronic Fund Transfer Act. The changes will close loopholes in the existing fraud provisions that have developed as a result of advances in technology and criminal sophistication.

SECTION 1

This section amends the Truth-in-Lending Act by adding a new section 129. The section would prohibit buying, selling, transferring or obtaining credit card account numbers with the intent to defraud or with a purpose other than a legitimate business purpose. Both civil and criminal penalities for a violation are provided by existing provisions contained in sections 130 and 112, respectively.

The language is intended to cover fraudulent schemes where a criminal "deals in" or obtains account numbers. It would include, for instance, the obtaining of an account number directly from the cardholder over the telephone or in person in order to use that number to incur fraudulent charges. It would also include obtaining numbers for similar purposes from sales receipts or carbons obtained collusively or by theft from merchants, and it would prohibit selling of lists of account numbers for fraudulent purposes. The account numbers improperly sold or disseminated may be in any form including electronic signal, magnetic tape or in any other oral or written form.

The section contains broad jurisdictional tests of affecting interstate or foreign commerce or using any instrumentality of interstate or foreign commerce. These standards are the same as those contained in other portions of the Act. The intent of the language is to give the broadest constitutionally permissible reach. This means that its reach would be limited only as may be required by the Constitution.

The section requires that the criminal activities be conducted with a purpose other than a legitimate business purpose involving credit card accounts, cardholders or the credit card system. This requirement is designed to ensure that innocent and legitimate dissemination of account numbers will not be affected. Thus, for example, merchants may continue to take telephone or mail orders charged to credit cards. In addition, account numbers may be used for many other legitimate purposes, including credit reporting, authorizations, billing and collection activities.

SECTION 2

This section makes an amendment to Section 134 of the Truth-in-Lending Act by adding a definition of the term "credit card" as used therein. The intent of this amendment is to close enforcement loopholes that may have developed since the enactment of the current statutory provisions. For example, the amendment would change the holding of one court that fraudulent misuse of an account number did not constitute the misuse of a "credit card." It defines credit card broadly to include any means of access that would permit a person to obtain credit or to initiate an extension of credit.

The definition explicitly includes both actual and fictitious account numbers. Thus, the statute's prohibitions will cover both the misuse of actual account numbers and the creation of fictitious numbers.

A code or other means of access is covered by the definition if it can be used alone or in conjunction with another "credit card" to obtain credit. This will cover, for example, personal identification numbers (PINs) which are used to activate a plastic card.

Finally, some of the subsections of Section 134 contain dollar amount minimums to trigger liability. The amendment makes clear that these dollar value tests are met by looking to one or more transactions using one or more credit cards. Therefore, a person cannot escape liability, for example, by using ten different counterfeit cards to make fraudulent purchases of $900 each or by using one credit card to make twenty purchases of $200 each.

SECTION 3

This section adds a new section 922 to the Electronic Fund Transfer Act in order to include language similar to that added to the Truth-in-Lending Act by Section 1. The comments above apply equally to this section.

SECTION 4

This section amends the definition of "debit instrument" contained in Section 916(c) of the Electronic Fund Transfer Act. The language builds on the existing definition now contained in 916(c) and is similar to that added to the Truth-in-Lending Act by Section 2. In this section, too, the comments made above are equally applicable.

In addition, the new definition makes clear that the criminal provisions of Section 916 apply to all debit accounts and not just to those established primarily for personal, family or household purposes.

Senator **HAWKINS**. Thank you, Mr. Alexander.

Mr. Branam.

STATEMENT OF JAMES R. BRANAM, JR., SENIOR VICE PRESIDENT, SOUTHEAST SERVICES, INC., MIAMI, FLA., ON BEHALF OF FLORIDA BANKERS ASSOCIATION

[Complete statement follows:]

TESTIMONY OF JAMES R. BRANAM, JR., THE FLORIDA BANKERS ASSOCIATION.

I am James R. Branam, Jr., Senior Vice President of Southeast Services, Inc., an affiliate of Southeast Bank, N.A., in the state of Florida. I am here today representing the Florida Bankers Association as Chairman of its Bank Card Committee. Thank you for the opportunity to appear before this subcommittee. My objective is to inform you of the tremendous losses that are being absorbed by the Florida Banks today as a result of fraud perpetrated with Bank credit cards.

Credit card fraud has increased at an alarming rate throughout the nation over the last three years. As a tourist and highly transient area and as the gateway to Latin America, the criminal element has focused on Florida as a base of operations establishing it as number two in the nation in Bank credit card fraud losses. In 1982, there was over $12 million in fraud losses perpetrated in Florida alone. That figure was exceeded only in the state of New York. This figure is a 542 percent increase over the losses sustained in 1979 just three years prior. The $12 million that I refer to is only bank card fraud and does not include the millions of dollars lost collectively by American Express, Diners Club, the oil companies and other credit card issuers.

The primary reasons for the dramatic increase in credit card fraud are:

The opportunities are great for the criminal element.—Due to the nature of the credit card business, it is prone to exploitation. Three to four years ago, the average credit card fraud perpetrator was a small time thief who used lost or stolen cards to buy merchandise and resell it at flea markets. Today the perpetrators are well organized in groups with access to stolen embossing machines and equipment to manufacture counterfeit cards or to alter legitimate ones. The groups have organized business structures similar to the illegal narcotics business and other organized crime. They have a large network of underground contacts from New York to Miami to Los Angeles. Miami in particular is susceptible due to the connections in narcotics and other illegal activities flowing through from Latin America. It is therefore easy for the groups to find willing participants, exepcially aliens, to join in the schemes. These networks grow quickly as satellite and independent groups learn the schemes.

The risks are minimal.—This type of criminal activity is normally non-violent because there is no need to carry a weapon. Additionally, the chances of being caught are low relative to other types of crime.

The penalties are practically non-existent.—The laws do not adequately cover all facets of the credit card frauds of today. The law enforcement agencies and judicial processes focus on violent and drug related crimes. It is difficult for authorities to make cases but if prosecution does occur, probation follows and the criminals are back in action within a short period of time.

LINKS TO NARCOTICS AND OTHER ILLEGAL ACTIVITIES

The local law enforcement agencies have linked some of the investigated fraud cases to narcotics dealers. It is documented that some credit card fraud organizations are using the illegally gained funds to finance narcotics and other illegal operations. Many of the cases are connected to individuals with operations in other states, particularly New York, as well as the Caribbean and Latin American countries.

SCHEMES AND SCAMS

There was a recent arrest made of a Latin alien in Miami as the result of a month long investigation by the Secret Service. When the Secret Service agents obtained a warrant to enter a home to confiscate approximately $250,000 in counterfeit U.S. Currency, they found over 100 White Plastic and Counterfeit credit cards. Some of these cards had been used in recent fraud schemes in New Jersey.

One of the organizations that has been operating in South Florida off and on since 1979 is a Nigerian group. This group is made up of Nigerian Nationals who enter our country under student visas allegedly for the purpose of study. Investigations reveal that these people have "studied" prior to entering the United States. Their "studies" consist of learning how to complete credit card applications with spurious information. Their U.S. organization supplies the participants with personal information on individuals with a high net worth. They use this information to fraudulently complete the credit applications. This group has also been involved in worthless check and counterfeit travelers checks schemes, and the exportation of stolen automobiles rented with the credit cards.

Another organization of aliens operating in South Florida is a Dominican group. These are Dominican Nationals involved in counterfeit schemes and because of their non-resident status, their operation is difficult to investigate.

During 1982, two brothers, who were Mariel boatlift refugees, established a scam involving several gasoline stations. The two brothers would threaten station attendants with bodily harm if they did not participate in the scheme. The scam caused thousands of dollars in losses to the banks. After an extensive undercover operation, the Metro Dade County police were able to break up the ring. The two brothers were never prosecuted as one witness was murdered and the other left the country.

One small merchant in Miami processed over $160,000 in bogus credit card receipts in a three month period. The operators of the boutique were Mariel boatlift refugees. The operation discontinued when one of the operators was murdered and the other disappeared.

WHITE PLASTIC [1]

White Plastic Schemes require the involvement of a collusive merchant. These schemes began in New York in 1980 and then exploded in South Florida in early 1982. The fraud groups contacted many merchants offering them an easy way to make some quick dollars with little or no risk. The merchants would be provided with blank plastics not issued by banks but containing good account numbers and legitimate names embossed on the cards. The plastics are used to imprint bogus sales slips to be deposited at the banks. The account numbers and names are obtained in various ways, including those provided by merchant clerks who handled valid transactions and retained the carbons with the account information. Many merchants in the Miami area were susceptible to participating in the scheme as their businesses that were formerly legitimate were struggling with low sales and minimal profits.

A month long "sting" operation by undercover law enforcement officers in Miami climaxed with the arrest of three individuals implicating 63 merchants in a white plastic scheme in July of 1982. A similar undercover operation was run in the Ft. Lauderdale area for a number of months ending in arrests of 32 merchants who had bilked the banks for $2 million in a year. The arrests made didn't stop the fraud in South Florida, they only slowed it down.

There are literally hundreds of stories similar to these bulging our loss files. In many cases, the use of extortion has been documented. In the New York banks there are many more with similar stories, some files containing connection to the "families" in organized crime.

The fraud losses sustained are a portion of the high cost of doing business in the credit card industry and are passed on to the consumer. It is estimated based on statistics taken from selected Florida Banks that the annual fraud costs for each credit card account maintained on the books is now up to $5.08 vs $.98 in 1978, a five fold increase.

CONSUMER ABUSES

During 1982, the banks in Florida, as well as the rest of the country, experienced an unusual problem with a credit card registration service based in the state. The company maintained a phone solicitation staff service. Although many of the consumers declined the offer, the company billed them for the service. The result was an enormous number of consumer complaints. This company obtained the consumer account lists from various sources including merchants where credit cards had been used in sales transactions. Actions were taken by the Visa and MasterCard associations and the Florida Bankers Association to control this type of consumer abuse within the industry.

The remaining problem is the need for laws to cover the illegitimate dissemination of account numbers and lists. It should be recognized by draftees of legislation addressing the legal issue that the industrys' legitimate use of account information should be preserved.

---

[1] White plastic is a term used in the credit card industry referring to a piece of plastic that is usually uncolored, has no bank name, logo or other identifying features but is embossed with a legitimate cardholders name and valid account number. The "white plastic" fraud is usually classifed as counterfeit for loss reporting purposes.

SUMMARY

Today we are dealing with drastically increased incidents and losses in bank card fraud as opposed to 3 years ago. We are also dealing in the main with a 1983 criminal element that is much more knowledgeable, organized and brazen than the petty thief of the 1970's. Large numbers of these perpetrators are aliens, making arrests and prosecution even more difficult without assistance from Federal agencies. The problem is that we are attempting to deal with 1980's criminals with inconsistent state laws written in the 1960's and Federal laws written in the early 1970's effective at that time but ineffective in today's environment.

It is the concensus of the Florida Bankers, as well as many local law enforcement officials, that in order to reduce the increasing upward spiral of credit card fraud, these actions must occur:

The Bank Card Industry must focus attention and resources on developing new technology and methods to deter the criminal activities.

Legislative action must be taken immediately to update the State and Federal Statutes to provide the law necessary to deal with the 1980's credit card criminal.

The Federal law enforcement agencies must be responsive and give the banks and local law enforcement agencies assistance, expecially where the schemes are National and International in scope.

The first action is well underway through the efforts of the American Bankers Association, MasterCard International, Visa International and at the state bankers association level. We desperately need your assistance on the second two actions.

Senator **Hawkins**. Thank you, Mr. Branam.

Mr. Neumann, in the interest of time, your full statement is very full, is there anyway you can summarize it? This is your summary, I understand, but is there anyway you could skip through that and give us the important portions at this time? We will have the full statement in the record so we can have some time for questions?

STATEMENT OF WILLIAM NEUMANN, VICE PRESIDENT FOR SECURITY, VISA INTERNATIONAL

Mr. **Neumann**. Madam Chairman and members of the subcommittee, I am William D. Neumann, vice president of Visa International in charge of security. I am appearing today on behalf of Visa U.S.A. Inc., a nonstock membership corporation which administers the Visa Card and Traveler's Cheque program throughout the United States. Our membership includes more than 13,000 commercial banks, savings banks, savings and loan associations, and credit unions that participate in the Visa program.

As of the end of 1982 the Visa "blue, white, and gold" card was carried by approximately 66.8 million individuals and accepted at nearly 2 million merchants outlets and 52,000 member offices all over the country. For 1982, the total dollars volume of the Visa Card system in the United States was approximately $38.5 billion.

On behalf of the vast membership of Visa, I would like to thank you, Madam Chairman, for convening these timely hearings to discuss the alarming increase in the incidence of credit card fraud and to review the current statutory provisions that provide criminal penalties in connection with the fraudulent use of these payment devices. Visa believes strongly that legislation is badly needed to stem the ever-increasing losses being suffered in this area.

THE SCOPE OF THE PROBLEM

Over the past few years, the fraudulent use of bank cards and travel and entertainment cards has spiraled to incredible heights. Its growth has been far out of proportion to the increase in the legitimate use of these cards. To illustrate the nature and scope of the problem, it is helpful to look at just one of its aspects, counterfeiting.

Worldwide card industry losses from counterfeiting alone were $15 million in 1981. In 1982, these losses soared to over $50 million, an increase of over 330 percent in 1 year alone. Of these worldwide losses, 94 percent were suffered in the United States. For the Visa system, counterfeit losses climbed from about $750,000 in 1981 to almost 15 times as much or nearly $11 million in 1982.[1]

Losses from counterfeiting are only one facet of the problem. In addition, Visa suffered general fraud losses of $69.3 million for 1982. About 36 percent of fraud losses involves stolen cards, with an average loss per card of $650. Lost cards are next, accounting for 29 percent of the dollar losses and an average dollar loss of about $1,000. Cards not received in the mail comprise the third largest category. This problem causes about 18 percent of the dollar losses, with an average loss per card of almost $2,000.

About two-thirds of fraud dollar losses result from purchases made before the issuer has any reason to believe that the card is being used fraudulently and has a chance to report it to authorization centers and merchants.

HOW FRAUD IS PERPETRATED

It may interest the members of this subcommittee to know how fraud is perpetrated. The Achilles' heel of the bank card is its embossed account number. Perpetrators obtain a good account number and emboss it on a counterfeit card, a plain piece of white plastic, or reemboss it on a lost or stolen card. This so-called new card can then generate hundreds of dollars of purchases and cash advances before it is blocked by the issuer. We have seen actual cases in which a hard-working fraudulent user could use a single card for $10,000 in phony transactions. On the street these cards can be bought illicitly for about $200.

Early criminal activity centered on lost and stolen cards, and then moved to manual alteration. The next stage in the evolution of card fraud was the development of far more sophisticated schemes including those involving counterfeiting and white plastic. "White plastic" is a term that refers to regular size, plain, blank plastic cards that are embossed with an account number, cardholder name, and expiration date. Clearly, these cards could not be used with legitimate businesses. Collusive merchants accepting the cards make their money by submitting phony sales records to the bank.

Most counterfeiting and card alteration activities are the work of organized gangs that operate with impunity across State lines, drain millions of dollars weekly from the economy, apply proceeds from their card activities to other types of crimes—notably drug and firearms dealings—and cause deadly violence.

One of the largest multifaceted card fraud operations perpetrated to date took place in the south Florida area. Losses in Dade

---

[1] These figures relate only to the losses. The operation costs add about 50 percent to those losses.

County, Fla., exceeded $10 million. The scheme utilized account information originating with issuing financial institutions based in Latin America. Cardholder information came from corrupt employees of hotels, restaurants, and car rental companies. As a result, the fraud had an impact on citizens from all over the United States and the United Kingdom who had never even visited the Miami area.

Another case that arose in New York involved the manufacture of over 200,000 counterfeit cards.

Although there have been arrests of some very sophisticated criminals, this has not stemmed the tide in counterfeit fraud losses to the industry. The cases reported to date represent only the tip of the iceberg and do not reflect a number of organizations continuing to operate and others as yet undetected.

CONGRESSIONAL ACTION NEEDED: A TWO-PRONGED APPROACH

The present magnitude of this problem and its potential call for congressional review of current laws protecting the public from fraud. Those that issue the cards and those that accept them bear the immediate brunt of the losses, but they are not the real victims. It is intuitively clear that ultimately fraud losses are paid by cardholders, in the form of higher costs of credit and merchandise.

Federal action is indeed needed. We believe that the scope and nature of this problem make a Federal response essential. The States generally do not have statutes that deal effectively with the issue. In addition, there are numerous reasons that command a Federal response.

First, and perhaps most important, the criminal behavior involved here places into jeopardy the entire national payments system.

Second, the activities generally are interstate in nature and tend to shift geographically based on the degree of industry and prosecutorial pressure exerted in major crime areas.

Third, and finally, there has been a longstanding role of the Federal Government in connection with debit and credit card activities.

In short, a timely and effective legislative response can be forthcoming only from Congress.

We believe that the problem now facing our industry must be addressed through a two-pronged legislative approach.

The first aspect involves a comprehensive provision to be included in the criminal title of the United States Code, Title 18. Enforcement efforts can be enhanced by a comprehensive law located in this portion of the United States Code. This will give Federal investigators and U.S. Attorneys specific guidance in card fraud investigations and prosecutions, and close gaps through which clever operators are able to slip. This is also consistent with the current framework of Federal criminal statutes that covers bank robbery, embezzlement, and similar crimes.

The card industry is therefore proposing comprehensive card fraud legislation creating a new chapter in the criminal portion of the Code that would provide penalties for the fraudulent use, possession or counterfeiting of various payment devices. It would include new provisions that address existing loopholes and areas of new and evolving card criminality.

We respectfully urge the Members of this subcommittee and the committee as a whole to support our effort to obtain a comprehensive Federal criminal statute. We are greatly encouraged, Madame Chairman, by indications that you are prepared to lend your support to such a measure.

While we are working with both House and Senate Judiciary Committees for the enactment of a comprehensive Title 18 bill, we also believe that certain limited changes should be incorporated in present law through amendments to the Truth-in-Lending and Electronic Fund Transfer Acts. The intent of these amendments is to close enforcement loopholes that may have developed since their enactment. They would amend these Acts by adding a definition of the terms "credit card" and "debit instrument" respectively, as the terms are used in certain sections of those statutes.

We believe that this two-pronged approach will provide the Federal criminal law framework necessary to address the evolving criminality now inflicting damage and costs on the payment system and the businesses and consumers who use it.

ACCOUNT NUMBER INFORMATION DISSEMINATION: AN AREA OF CRITICAL IMPORTANCE TO THE CARD INDUSTRY

In addition to these two amendments, responding to concern expressed by some committee members, we also have prepared suggested statutory language dealing with the dissemination of account number information.

Specifically, the section relating to dissemination would amend the Truth-in-Lending Act by adding a new section. It would prohibit buying, selling, transferring or obtaining credit card account numbers with the intent to defraud or with a purpose other than a legitimate business purpose. This latter element is designed to insure that legitimate dissemination of account numbers will not be affected. Both civil and criminal penalties for a violation are provided by existing provisions.

In order to protect legitimate business activities, we would strongly recommend that any Federal legislation be structured in a manner similar to that contained in Appendix G to our written statement. We would be pleased to work with appropriate staff members in devising legislation that will deal effectively with troublesome practices while safeguarding the legitimate workings of the credit marketplace.

CONCLUSION

In conclusion, the pervasive and growing use of plastic cards and related access mechanisms is ushering in a world wide system of electronic funds exchange. These payment mechanisms hold the potential for allowing consumers to use their assets anyway they see fit, instantly, anywhere in the world and at any time of day. They hold the key to expanding their freedom by expanding their financial flexibility.

If this new approach to financial services is to be implemented successfully, it must be able to develop free of the existing threat of widespread criminality not effectively addressed under—and, thus, not deterred by—the Federal criminal justice system. Visa and others in the card industry respectifully urge Congress to give immediate consideration to the proposals that I have addressed today. Thank you.

[Complete statement follows:]

TESTIMONY OF
VISA U.S.A. INC.
BEFORE THE
COMMITTEE ON BANKING, HOUSING
AND URBAN AFFAIRS
SUBCOMMITTEE ON CONSUMER AFFAIRS
UNITED STATES SENATE

HEARINGS ON THE NATURE AND SCOPE OF CREDIT AND DEBIT CARD FRAUD AND RELATED ISSUES

Madame Chairman and Members of the Subcommittee, I am William D. Neumann, Vice President of Visa International in charge of security. I am appearing today on behalf of Visa U.S.A. Inc., a non-stock membership corporation, incorporated under the laws of the State of Delaware, which administers the Visa Card and Travelers Cheque Program throughout the United States. The membership of the corporation is comprised of approximately 13,000 commercial banks, savings banks, savings and loan associations, and credit unions that participate in the Visa program.

As of the end of 1982 the Visa "Blue, White and Gold" card was carried by approximately 66.8 million individuals and accepted at nearly 2 million merchant outlets and 52,000 member offices all over the country. For 1982, the total dollar volume of the Visa Card system in the United States was approximately $38.5 billion.

On behalf of the vast membership of Visa, I would like to thank you, Madame Chairman, for convening these timely hearings to discuss the alarming increase in the incidence of credit card fraud and to review the current statutory provisions that provide criminal penalties in connection with the fraudulent use of these payment devices. Visa believes strongly that legislation is badly needed to stem the ever-increasing losses being suffered in this area. We would like to emphasize, Madame Chairman, that these losses are not borne by Visa or others that perform an intermediary function but rather they are paid for by the consumers who actually use the system through increased prices for credit and the goods and services being purchased.

The Scope Of The Problem

Over the past few years, the fraudulent use of bank cards and travel and entertainment cards has spiraled to incredible heights, far out of proportion to the increase in the legitimate use of these cards. To illustrate the nature and scope of the problem, it is helpful to look at just one of its aspects, counterfeiting.

Worldwide card industry losses from counterfeiting alone were $15 million in 1981. In 1982, these losses soared to over $50 million, an increase of over 330 percent in one year alone. Of that amount, the United States accounts for about 94 percent of those losses or approximately $47 million.

For the Visa system, counterfeit losses climbed from about $750,000 in 1981 to nearly $11 million in 1982, an astounding increase of over 1,460 percent. Furthermore, despite stepped-up security operations, these losses are expected to at least double in 1983 to well in excess of $20 million. Counterfeiting losses sustained by Visa members in 1982 were seven times greater than the total counterfeit losses for the previous nine years. (See Appendix A.) A recent but limited survey by Visa indicates that counterfeiting per se constitutes just over 11 percent of the total fraud losses and generates an average dollar loss per counterfeit card of $1,000. (See Appendix B.) MasterCard and American Express also have sustained significant losses in this area.

Losses from counterfeiting are only one facet of the problem. In addition, Visa suffered general fraud losses of $69.3 million for 1982. Most fraud losses involve stolen cards (nearly 36 percent of the dollar losses with an average loss per card of $650). Lost cards are next, accounting for 29 percent of the dollar losses and an average dollar loss of about $1,000. Cards not received in the mail comprise the third largest category of loss. These are cards intercepted after they are mailed by Visa but before they are received by the actual accountholder. This problem causes about 18 percent of the dollar losses, with an average loss per card of almost $2,000. (See Appendix B.)

It is important to emphasize that the cards involved in these three categories of fraud that give rise to the highest losses -- lost cards, stolen cards, and "card not received" -- are often used at first for large dollar purchases. Once the perpetrator has used the card for amounts that he assumes approach the card's credit limit, the cards are used for smaller transactions, which do not require direct authorization. This continues until the account is blocked by the issuer. Essentially, "blocking" an account means that authorization and security mechanisms are set in place to prevent any further use of that account. It is at this point that the cards are recycled by the criminals, altered with new account numbers, and move into the "counterfeit" category.

About two-thirds of fraud dollar losses occur from purchases made before the issuer has any reason to believe that the card is being used fraudulently and reports it to authorization centers and merchants. Generally, this process takes about a week, but can take much longer than that for overseas accounts.

Although more than half of the fraudulent transactions involve less than $50, they account for only about 12 percent of total dollar losses. Transactions between $500 and $999, while comprising less than nine percent of transactions, actually account for more than a third of all dollar losses. Transactions of more than $1,000 account for only 1.3 percent on a transaction basis, but more than 16 percent of dollar losses. (See Appendix C.)

More than 93 percent of the fraud losses in the U.S. occur in 12 states. (See Appendix D.) It is interesting to note that major areas of card fraud, according to our preliminary review, appear to coincide with the locations of major, known organized crime families.

Almost 25 percent of all fraudulent transactions occur in department, variety and general merchandise stores, in transactions that involve an average amount of about $100. One-fifth of the percentage of dollar losses results from cash advances, made by banks for an average amount of about $600. (See Appendix E.)

Significantly, the average transaction amount of about $55 before the account is blocked drops to about $36 after the block date. This seems to suggest strongly that fraudulent users are aware of the card issuer "floor limits" and other authorization procedures that are used by the industry to police fraud.

How Fraud Is Perpetrated

The Achilles heel of the bank card is its embossed account number. Perpetrators obtain a "good" account number and emboss it on a counterfeit card, a plain piece of "white plastic," or reemboss it on a lost or stolen card.

This "new" card can then generate hundreds of dollars of purchases and cash advances before it is blocked by the issuer. Some investigators and informants have stated that an ambitious and hard-working fraudulent user could use a single card to make $10,000 in phoney transactions. On the black market these cards can be bought illicitly for about $200.

Fundamental to many of these schemes is obtaining good account numbers. Criminals do this in many ways, among them:

-- searching merchants' trash and recovering carbon sheets from card transactions. The account number, cardholder's name and expiration date are clearly legible;

-- buying stolen cards, frequently from prostitutes. The going rate is said to be $25 to $50;

-- getting short-term mail order or telephone order jobs;

-- learning the access code to a computerized credit reporting agency, or finding a confederate on the inside;

-- working for, or having a confederate who works for, a bank. A major fraud case in New York recently resulted in the arrest of four bank employees who were trafficking in account numbers from high-limit accounts; or

-- posing as a card company representative or another legitimate businessman over the telephone and persuading cardholders to recite their account numbers.

Once the perpetrators have account information, they simply emboss it on a piece of plastic. These efforts have gone through several identifiable stages as criminals have gained knowledge about both the card system and the mechanics of producing cards. In this area, as in others, it is possible to trace an acceleration and increase in sophistication of criminal activity as these elements work to keep up with industry changes calculated to thwart fraud.

Early criminal efforts centered on lost and stolen cards. The cards were used only until the reporting and listing processes involving lost and stolen cards were assumed to have caught up with them. This period of exposure was reduced as the industry responded with improved reporting and authorization systems. Discovering the brief period during which these cards were useable, criminals soon changed their approach.

The first efforts at manually altering credit cards involved "shave and paste." The "shave and paste" scheme, as it became known in the credit card industry, involves the removal of accountholder information embossed on the face of lost or stolen cards using a razor knife. New numbers removed from other credit cards are then glued onto the appropriate places on cards using a fast-drying epoxy cement. Initial attempts were addressed at changing the validation and expiration date lines, often using discarded, "expired" cards. In its final stage, the efforts moved to changes in the account number lines. While current methods of fraud make this early scheme appear crude by comparison, it is still being used today.

The next stage in the evolution of card fraud was the development of far more sophisticated schemes including those involving card counterfeiting and "white plastic." "White plastic" cards are plain plastic of the correct size to fit in the sales draft embossing equipment widely available in the marketplace. These blank cards are embossed with an account number, cardholder name and expiration date. This produces a plain white embossed card (white, because that happens to be the color in which the plastic used is produced) that does not have any issuer or card company logo. Clearly, these cards could not be used with legitimate businesses. They require the cooperation of an unscrupulous, collusive merchant. The merchant's role is to get a transaction authorization, and then submit a phoney sales record to the bank. These schemes require a capital investment for, among other items, embossing machinery. Top-of-the-line embossing machines, many of which have correcting keys allowing dis-embossing, sell for anywhere from $2,500 to $15,000 on the legitimate market, and three times as much in the counterfeit card market.

Some counterfeit or altered card use is the work of petty thieves working alone, but most counterfeiting and card alteration activities are the work of organized gangs. They operate with impunity across state lines, drain millions of dollars weekly from the above-board economy, apply proceeds from their card activities to other types of crimes -- notably drug and firearms dealings -- and cause deadly violence, doubtless sometimes involving innocent victims.

Card Fraud: A Case History

One of the largest multifaceted altered card/white plastic/counterfeit fraud operations perpetrated to date took place in the South Florida area. Losses in Dade County, Florida, exceeded $10 million. The scheme utilized account information originating with issuing financial institutions based in Latin America, primarily Mexico, Venezuela, Columbia, and Argentina. Also involved were accounts issued to South American nationals but maintained in United States dollars. This modus operandi took advantage of a three-month delay before the true cardmember's denial of the charges reached the issuer's domestic security departments for investigation.

Initially, the credit card industry applied a systems approach in authorizations in order to minimize fraud exposure, particularly in connection with Venezuelan accounts. The result demonstrated exactly how nimble these conspirators are, since, in response to this industry enforcement effort, they simply changed their focus to European cardmembers rather than those of Latin America. It was later determined that one source of cardmember information was a jewelry store in the Costa del Sol run by an organized crime capo from Sicily. As law enforcement and industry pressure grew, they again simply shifted their operations using United

States cardmember information to commit card fraud on the French Riviera and in Italy, Argentina, Venezuela, and Columbia.

Valid cardmember information came from corrupt employees of hotels (guest registration cards in Miami contained notations of passport numbers and South American police identity card numbers), restaurants and rental car companies. In the rental car instance, one rental agency served as a billing location for the entire country. As a result, the fraud had an impact on citizens from all over the United States and the United Kingdom who had never even visited the Miami area.

In 1982, other groups of organized criminals also were arrested in Southern Florida. Recently, 50 "collusive merchants" were identified and prosecuted in a joint effort by the credit card industry and local law enforcement authorities for their part in a continuing fraud scheme that was national in scope.

We will be happy to provide the committee with a confidential document providing a detailed description of major fraud cases that have been investigated to date.

The arrests of members of very sophisticated groups of criminals have not stemmed the tide in counterfeit fraud losses to the industry. The cases reported to date represent only the "tip of the iceberg" and do not reflect a number of organizations continuing to operate and others as yet undetected.

In many instances, successful federal prosecutions in cases like the one described above simply cannot be undertaken due to lack of meaningful and comprehensive federal statutes in this area. For instance, some believe that there is doubt as to the coverage of such items as the fraudulent use of "white plastic" and the unlawful possession of cardmember information and carbon copies of charge slips.

Congressional Action Needed: A Two-Pronged Approach

In the judgment of a unified credit card industry, the present magnitude of this problem and its potential for even more staggering increases warrant a Congressional review of laws protecting the public from fraud in connection with credit and debit cards. The problems are serious enough now to require special attention. The long-term potential for misuse of payment devices, given the current state of law, has far-reaching ramifications bearing on the integrity of the nation's payment system that increasingly involves credit and debit cards and related codes and numbers. We respectfully urge the Members of this Subcommittee to bear in mind that these pieces of plastic are tantamount to cash and their fraudulent use is directly analogous to the counterfeiting of U.S. currency.

Those that issue the cards and those that accept them bear the immediate brunt of the losses, but they are not the only victims. It is intuitively clear that ultimately fraud losses are paid by cardholders, as components of the cost of credit and merchandise. Moreover, there is evidence that most card fraud schemes are well organized, operate across state lines, very likely finance other more sinister illegal activities, and result in violence.

Federal Action Is Needed. We believe that the scope and nature of this problem make a federal response essential. While many states have statutes that can be construed to cover the fraudulent activities involved here, we have not discovered any that deal directly and effectively with the issue. This situation is particularly troublesome in light of the fact that criminal statutes by law must be construed strictly, thus occasioning some concern when these general statutes are stretched to cover the specific criminality under discussion here.

In addition to the lack of adequate state law, there are numerous reasons that commend a federal response. First, and perhaps most important, the criminal behavior involved here places into jeopardy the entire national payments system. This system, which is in no way limited by state boundaries, has increasingly developed into one based in substantial part on the use of credit and debit cards and related access mechanisms. The danger inherent in a lack of coverage at the federal level is that the system as a whole will be less secure and certain. Given the existence of a nationwide payment system, it is simply beyond the ability of any one or even several states to deal effectively with the problem.

Second, based on our experience with significant fraud cases, the activities generally are interstate in nature. With the high degree of organization of criminal efforts in this area, it is simply not possible to stop these efforts through state or local legislative action. Insofar as there are state statutes in existence, enforcement by states, cities or counties must stop at their jurisdictional limits while card fraud operations routinely operate across state and national boundaries. In addition, our experience has demonstrated conclusively that the problem tends to shift geographically based on the degree of industry and prosecutorial pressure exerted in major crime areas. Thus, for example, as enforcement efforts increase in New York and Miami, new outbreaks of crime are experienced in Phoenix and in other parts of the country that previously had not been major centers of crimes of this type.

Third and finally, there has been a long-standing role of the federal government in connection with debit and credit card activities. Comprehensive legislation adopted over a decade ago established federally-mandated rules on disclosure, billing error rights and substantive responsibilities. Almost five years ago Congress adopted comprehensive legislation to deal with electronic transfers. These statutes, implemented by extensive regulations adopted by the Federal Reserve Board, further demonstrate the significance historically given by Congress to the issues involved here.

In short, a timely and effective legislative response can be forthcoming only from Congress.

A Legislative Proposal. We believe that the problem now facing our industry must be addressed through a two-pronged legislative approach. The first aspect involves a comprehensive provision to be included in the criminal title of the United States Code, Title 18, to provide a complete response to the current problem. The second element would be limited but important changes to existing criminal provisions now contained in the Truth in Lending and Electronic Fund Transfer Acts.

1. A Comprehensive Response: Title 18. Existing federal laws placed obscurely in the Truth in Lending and Electronic Fund Transfer Acts are fragmented, contained in a

format different from other criminal laws and contain some troublesome loopholes. These laws have primarily a consumer-protection orientation and regulate commercial behavior, generally describing how businesses are to comply with disclosure, billing, collection, and other business procedures. Laws regarding intrinsically illegal activities, such as card counterfeiting, seem misplaced in this context.

The industry's experience with card fraud investigations has led to a conviction that enforcement efforts can be enhanced by a comprehensive law located in the criminal portion of the United States Code to give federal investigators and U.S. Attorneys specific guidance in card fraud investigations and prosecutions, and by closing gaps through which clever operators are able to slip.

In this regard, the leading card companies are proposing comprehensive card fraud legislation creating a new chapter in the criminal portion of the Code that, for the first time, would enable federal enforcement agencies and U.S. Attorneys to deal effectively with interstate manufacturing and trafficking in counterfeit or altered cards. (See Appendix F.)

Members of the law enforcement community who are unfamiliar with card fraud statutory provisions are not likely to turn to U.S. commercial titles to learn their provisions. Title 18 -- containing federal criminal provisions -- and not Title 15, is the book that is on their desks. Those who do know where to look to find the law now face a task which, while not impossible, still imposes a threshold barrier that may be significant for already overworked federal prosecutors and investigators. The provisions there rely heavily on case law and definitions that appear elsewhere in Title 15, making necessary a research effort that could be a barrier to action.

On the other hand, a new chapter in Title 18, covering "Payment Mechanisms," would provide all of the statutory information in one place that is necessary to build an effective case. The new chapter would define payment devices and fraudulent payment devices and provide penalties for their fraudulent use, possession or counterfeiting. It would bring under a single heading existing federal statutes dealing with card fraud as well as new provisions that address existing loopholes and areas of new and evolving card criminality.

There is ample precedent for such a proposal. Congress in 1948 modernized all existing criminal laws and combined many overlapping statutes under Title 18. Since then Congress has on numerous occasions rearranged the collection of criminal provisions in order to place them in Title 18.

Examples include a number of provisions covering other types of fraud from Title 12 (banking) and Title 15 (commerce) to Title 18. Similarly, a variety of bank-related crimes are now included in Title 18 that originally had been placed in 12 U.S.C. §§ 583 through 588d.

Moreover, this proposal, which has the unanimous support of the major card companies, is consistent with the direction Congress is now taking in its current revision of the federal criminal code.

Placing card crimes within the criminal portion of the Code has an advantage beyond proper location. The approach also more clearly follows the regular order through which federal criminal laws are adopted, and gives a clear signal about the importance of this issue from the Congressional committees that provide funding and direction to the federal criminal justice system.

For all of these reasons, we respectfully urge the Members of this Subcommittee and the Committee as a whole to support our effort to obtain a comprehensive federal criminal statute. We are greatly encouraged, Madame Chairman, by indications that you are prepared to lend your support to such a measure. We hope that you and the other Members of this Committee will cosponsor legislation that we are hopeful will be introduced soon and assigned to the Senate Judiciary Committee.

2. Limited But Important Changes to Existing Statutes. While we are working with both House and Senate Judiciary Committees for the enactment of a comprehensive Title 18 bill, we believe that certain limited amendments should be incorporated in present law through amendments to the Truth in Lending and Electronic Fund Transfer Acts.

These provisions would amend Section 134 of the Truth in Lending Act and Section 916(c) of the Electronic Fund Transfer Act by adding a definition of the terms "credit card" and "debit instrument" respectively, as the terms are used in those sections. (See Appendix G.)

The intent of these limited amendments is to close enforcement loopholes that may have developed since their enactment. For example, they would change the holding of one court that fraudulent misuse of an account number did not constitute the misuse of a "credit card." The definitions explicitly include both actual and fictitous account numbers. Thus, the statute's prohibitions will cover both the misuse of actual account numbers and the creation of fictitous numbers.

Second, some of the provisions in the criminal sections of these Acts contain dollar amount minimums that must be met in order to trigger liability. The amendments would make clear that these dollar value tests are met by looking to one or more transactions using one or more credit cards.

Therefore, a person would not escape liability, for example, by using ten different counterfeit cards to make fraudulent purchases of $900 each.

We believe that this two-pronged approach -- a comprehensive new provision in Title 18 and limited amendments in current commercial laws -- will provide the federal criminal law framework that would address the evolving criminality now inflicting damage and costs on the payment system and the businesses and consumers who use it. We urge the Subcommittee to move quickly to adopt those portions of this suggested legislative program that fall within this Committee's jurisdiction.

Account Information Dissemination: An Area Of Critical Importance To The Card Industry

In addition to these two amendments, responding to concern expressed by some Members of the Committee, we also have included suggested statutory language dealing with the dissemination of account information.

Specifically, the section relating to dissemination amends the Truth in Lending Act by adding a new Section 129. This section would prohibit buying, selling, transferring or obtaining credit card account numbers with the intent to defraud or with a purpose other than a legitimate business purpose. Both civil and criminal penalties for a violation are provided by existing provisions contained in Sections 130 and 112, respectively.

The section provides that the activities be conducted with a purpose other than a legitimate business purpose involving credit card accounts, cardholders or the credit card system. This requirement is designed to ensure that legitimate dissemination of account numbers will not be affected. The language used follows that used in the Fair Credit Reporting Act, adopted by Congress in October, 1970. That statute and this language are familiar to creditors, the courts and the regulatory agencies alike. For more than a decade, this test has been used successfully in the credit reporting area. It would serve equally well in this area.

We believe it is essential to emphasize that caution must be exercised with respect to any legislation structured to restrict the dissemination of account numbers, or any other account information. While we can support, and in fact would welcome, narrowly drafted legislation to deal with the improper sale of account numbers, any restrictions on the legitimate business use of account numbers or other information would disrupt the entire payment and credit granting system and would severely inconvenience the consumer in doing business in today's mobile society.

Obviously, the account number is necessary to link the transaction and the account to the consumer initiating the transaction. It is a cardholder's account number along with his or her name and card expiration date that is imprinted on the sales draft which is passed or the the merchant bank, routed to the card issuing bank and ultimately billed to the consumer's account. During the course of the merchant transaction the account number is also used to obtain authorization for a specific purchase.

We also have instituted at the merchant location a system whereby the merchant reviews a negative file to identify any account numbers linked to bad accounts. This system is vital to the card industry's security operations and provides a mechanism to help control fraud when we know a specific account has been blocked. Any restrictions on this use of account numbers would be counterproductive and further inhibit the industry's ability to control fraud.

It is also important to the credit granting process that credit reporting agencies retain access to account information including account numbers. These agencies are very important to the card issuers in checking the creditworthiness of applicants, and the credit granting process would be seriously impaired if this information flow were disrupted.

Our members must also have the authority to transfer account information in the normal course of buying and selling card portfolios. More and more, as depository institutions elect to move in and out of the card business, entire portfolios are being transferred between institutions. Unless legislation in this area is carefully structured, institutions would be unable to act on these types of business decisions without severely disrupting the system.

We have also seen a rapid increase in the amount of mail and telephone orders of merchandise. A large sector of special merchandising houses has sprung up to meet these demands and they continue to provide consumers a convenient method of purchasing the goods that they offer.

In order to protect these and other types of legitimate business activities, we would strongly recommend that any federal legislation be structured in a manner similar to that contained in Appendix G. We would be pleased to work with appropriate staff members in providing our views as to the shape and scope of legislation that will deal effectively with troublesome practices while safeguarding the legitimate workings of the credit marketplace.

What The Industry Is Doing

In seeking federal legislation, the credit card industry does not mean to suggest that it must lessen its vigilant efforts to curb this problem. In fact, all the major card companies have -- and are rapidly expanding --

aggressive programs to fight card fraud, ranging from developing card designs that inhibit counterfeiting and alteration to electronic authorization systems at the point of transaction.

In addition to these preventative programs, the card companies participate actively in law enforcement investigations into card fraud cases. In fact, one Ft. Lauderdale, Florida, investigation, which resulted in the arrest of more than 30 unscrupulous merchants, began with information provided to Visa through the use of an informant. The informant, still working with law enforcement on other cases, was found in the course of the investigation of a big New York-area card fraud operation. Through the efforts of Visa, the informant was made available to the Florida authorities, and later to authorities in another part of the country to work on yet other investigations.

Visa also initiated another investigation in the same area by presenting a case it had investigated to a joint law enforcement agency.

On other levels, Visa:

-- has commissioned SRI International to develop a program to help card issuers and merchants resist fraud;

-- has organized an ad hoc security adviser group of Visa members to examine and critique Visa security efforts;

-- has begun development of a computerized means of quickly identifying geographical "hot spots" of card fraud, which will allow a concentration of fraud-fighting measures, when and where they are needed most;

-- is developing the means to computer-authorize every transaction, via electronic terminals at the point of transaction; and

-- has initiated an integrated global security system made up of professionals in the area of prosecution and law enforcement to assist our members and the criminal justice system.

We are also active participants on committees of the American Bankers Association and other trade associations that are providing merchants and card issuers seminars on how to fight fraud. Furthermore, Visa recently revised its operating regulations to put in place additional safeguards for protecting the cardholders' account numbers and to give our members specific guidelines as to their proper dissemination.

Conclusion

The pervasive and growing use of plastic cards and related access mechanisms is ushering in a worldwide system of electronic funds exchange. These payment mechanisms hold the potential for allowing consumers to use their assets any way they see fit, instantly, anywhere in the world and at any time of day. They hold the key to expanding their freedom by expanding their financial flexibility.

This is not futurism. The technology is here now. Judging by their acceptance of automated teller machines, consumers are ready and eager to move into this new era. By 1986, as an example, Visa will have established a global network of at least 8,000 automated teller machines, giving cardholders immediate access to their financial accounts worldwide.

If this new approach to financial intermediation is to be implemented successfully, it must be able to develop free of the existing threat of wide-spread criminality not effectively addressed under -- and, thus, not deterred by -- the federal criminal justice system. It is to control this situation and to maintain security over the electronic funds transfer system and the entire national payments system that Visa and others in the card industry urge Congress to give immediate consideration to the proposals that I have addressed today.

We appreciate having had the opportunity to share our views with you. I would be happy to answer any questions that you may have.

APPENDIX A

GROWTH OF COUNTERFEITING
Visa International

1972-73 . . . . . $12,000

1973-74 . . . . . $4,600

1974-75 . . . . . $10,800

1975-76 . . . . . $27,200

1976-77 . . . . . $26,700

1977-78 . . . . . $31,700

1978-79 . . . . . $78,700

1979-80 . . . . . $516,000

1980-81 . . . . . $740,000

1981-82 . . . . . $10,920,000

1982-83 (est.). . $20,000,000

APPENDIX B

FRAUD BY TYPE

Visa International

Type	% of $ Loss	Average Dollar Amount
Lost	29.2%	$1,047
Stolen	35.9	650
Card not received	18.7	1,919
Counterfeit	11.2	1,102
all other	5.0	--

APPENDIX C

FRAUD TRANSACTIONS BY SEVERITY AND FREQUENCY

Transaction Amount	% of Transactions	% of Losses
Under $50	58.1%	12.1%
$50 to $149	14.1	7.3
$150 to $249	6.7	7.5
$250 to $349	5.2	9.0
$350 to $499	5.9	14.5
$500 to $999	8.7	33.5
$1,000 and over	1.3	16.1

APPENDIX D

COUNTERFEIT LOSSES BY LOCATION

Visa International

Location	% of Transactions	Dollar Value of Transactions
New York City	28.2%	$2,555,397
New York State	14.5	1,309,838
Florida	19.1	1,728,231
New Jersey	8.1	729,295
California	5.2	470,757
Massachusetts	4.0	360,335
Pennsylvania	3.2	293,730
Connecticut	2.5	229,613
Texas	1.6	144,645
Illinois	1.1	100,251
Michigan	1.0	89,673
Virginia	1.0	88,526
Nevada	0.9	85,722

APPENDIX E

COUNTERFEIT BY TYPE OF TRANSACTION

Visa International

Transaction Type	% of Transaction	% of $ Losses	Average Amount
Cash advances	5.7%	20.8%	$624
department, variety & general stores	23.2	13.9	102
radio, stereo, tv	4.8	11.0	393
clothing	6.9	4.8	118
jewelry	1.2	4.5	611
restaurants	7.1	2.3	55
shoe stores	4.7	2.2	81
airlines	1.4	1.9	235
furniture	0.4	1.6	614
hotel/motel/resort	2.5	1.5	102
camera/photography	1.5	1.5	178
travel agencies	0.2	1.3	930
household appliances	0.5	1.3	407
auto parts	0.8	1.2	271
drug stores	3.8	1.1	50
wire transfer/ money orders	0.2	0.9	930
unkown (illegible drafts)	21.7	18.0	141
remainder	13.4	10.2	100

APPENDIX F

5/06/83

DRAFT

[To add a new Chapter to Title 18 to proscribe various activities in connection with payment devices.]

Chapter 76

Payment mechanisms

§ 1561 Definitions

As used in this chapter --

(1) "payment device" means any card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another payment device, to obtain money, goods, services, or any other thing of value, or to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2) "fraudulent payment device" means (A) any payment device or a facsimile, likeness, or similitude of a payment device that is counterfeit, fictitious, altered, forged, falsely made, lost, stolen, incomplete, expired, revoked, cancelled, fraudulently obtained, or obtained as part of a scheme to defraud, or (B) any invoice, voucher, sales draft, or other reflection or manifestation of such a device.

(3) "financial institution" means an institution with deposits or accounts insured by the Federal Deposit Insurance Corporation, the Federal Savings and Loan Insurance Corporation, or the National Credit Union Administration.

§ 1562 Fraud

(a) Whoever knowingly buys, receives, conceals, possesses, furnishes, exchanges, transfers, sells, delivers, or transports one or more fraudulent payment devices or any constituent part, component, or aspect thereof

(1) with unlawful or fraudulent intent;

(2) knowing the device to be a fraudulent payment device; and

(3) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using an instrumentality of interstate or foreign commerce, or (C) with a fraudulent payment device, or any constituent part, component, or aspect thereof, that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved 25 or

more fraudulent payment devices or constituent parts thereof, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(b) Whoever knowingly uses one or more fraudulent payment devices to obtain money, goods, services, or any other thing of value aggregating $1,000 or more in value in any one or more transactions occurring in any twelve-month period

(1) with unlawful or fraudulent intent;

(2) knowing the same to be a fraudulent payment device; and

(3) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using an instrumentality of interstate or foreign commerce, or (C) with a fraudulent payment device, or any constituent part, component, or aspect thereof, that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved money, goods, services, or any other thing of value aggregating $20,000 or more in value in any one or more transactions

occurring in any twelve-month period, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(c) Whoever knowingly buys, receives, conceals, possesses, furnishes, exchanges, transfers, sells, delivers, or transports money, goods, services, or any other thing of value aggregating $1,000 or more in any one or more transactions occurring in any twelve-month period

(1) with unlawful or fraudulent intent;

(2) knowing the same to have been obtained with one or more fraudulent payment devices; and

(3) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using an instrumentality of interstate or foreign commerce, or (C) with money, goods, services, or any other thing of value that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved money, goods, services, or any other thing of value aggregating $20,000 or more in any one or more transactions

occurring in any twelve-month period, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(d) Whoever knowingly buys, receives, conceals, possesses, furnishes, exchanges, uses, transfers, sells, delivers, or transports any actual or fictitious account information pertaining to a payment device or a fraudulent payment device, including without limitation account holders' names, account numbers, expiration dates, and identification or other access codes,

(1) with unlawful or fraudulent intent; and

(2) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) with respect to information that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved information pertaining to 25 or more payment devices, fraudulent payment devices, or accounts, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(e) Whoever attempts to commit, or solicits another to commit, any of the offenses described in this section shall be subject to the same penalty as attaches to the offense attempted or solicited.

§ 1563 Counterfeiting

(a) Whoever

(1) (A) falsely makes, forges, counterfeits, or alters any payment device or otherwise causes a payment device to become a fraudulent payment device, or (B) makes, devises, fabricates, or develops a fraudulent payment device, or any device or thing that can be used as, or in lieu of, a payment device, or that is or may be any constituent part, component or aspect thereof;

(2) with unlawful or fraudulent intent; and

(3) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) with a payment device, fraudulent payment device, device or thing that can be

used as, or in lieu of, a payment device, or any constituent part, component, or aspect of any of these that has moved in, has been part of, or constituted or with the intent that it will move in, will be part of, or constitute interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved 25 or more such devices or things, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(b) Whoever passes, utters, publishes, sells, brings into the United States, keeps in possession, or conceals any falsely made, forged, counterfeited, or altered payment device or any other fraudulent payment device or any constituent part, component, or aspect thereof,

(1) with unlawful or fraudulent intent; and

(2) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) with any such payment device, fraudulent payment device, or any constituent part, component, or aspect thereof that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved 25 or more fraudulent payment devices or constituent parts thereof, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(c) Whoever buys, sells, uses, exchanges, transfers, receives, or delivers any falsely made, forged, counterfeited, or altered payment device or any other fraudulent payment device or constituent part, component, or aspect thereof,

(1) with the unlawful or fraudulent intent that the same be passed, published, or used as true and genuine; and

(2) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) with any such payment device, fraudulent payment device, or any constituent part, component, or aspect thereof that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved 25 or

more fraudulent payment devices or constituent parts thereof, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(d) Whoever, with unlawful or fraudulent intent, obtains control, custody, or possession of any equipment or mechanisms used or that can be used to make, devise, fabricate, or develop fraudulent payment devices or any constituent part, component, or aspect of a device or thing that becomes or can be used as, or in lieu of, a payment device,

(1) by making, devising, fabricating, or developing a fraudulent payment device including any constituent part, component, or aspect of a device or thing that can be used as, or in lieu of, a payment device; and

(2) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) using such equipment or mechanisms that have moved in, been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(e) Whoever attempts to commit, or solicits another to commit, any of the offenses described in this section shall be subject to the same penalty as attaches to the offense attempted or solicited.

§ 1564 Presumption

For purposes of this chapter, the possession of eight or more fraudulent payment devices or of account or other information pertaining to eight or more fraudulent payment devices shall create a presumption that unlawful or fraudulent intent existed with respect to a specified act or activity, but such presumption shall be rebuttable.

§ 1565 Application for a payment device*

Whoever knowingly makes any false statement or report, or willfully overvalues any land, property or security, for the purpose of influencing in any way the action of any person (1) that moves or engages in interstate or foreign commerce or whose transactions in this regard affect interstate or foreign commerce and (2) that offers or issues payment devices, upon any application, advance, withdrawal, discount, purchase, purchase agreement, repurchase agreement, invoice, voucher, sales draft, commitment, or loan, or any change or extension of any of the same, by renewal, deferment of action or otherwise, or the acceptance, release, or substitution of security therefor, shall be fined not more than $5,000 or imprisoned not more than two years, or both.

---

* A preferable alternative to including this provision as a separate section here might very well be to add it as a new subsection (b) to existing 18 U.S.C. § 1014, which this section follows very closely.

§ 1566 Repeated violations

Whoever engages in any activity proscribed in sections 1562 or 1563 after one or more prior convictions for him under either of these sections have become final shall be fined not more than $20,000 or imprisoned not more than 20 years, or both.

APPENDIX G

DRAFT
5/05/83
Title 15

[A bill to amend the Truth in Lending Act
and the Electronic Fund Transfer Act.]

Sec. 1. The Truth in Lending Act (15 U.S.C. §§ 1601 *et seq.*) is amended by adding a new section to be designated section 129 to read as follows:

"Section 129. No person in a transaction affecting interstate or foreign commerce, or using any instrumentality of interstate or foreign commerce, shall buy, sell, furnish, exchange, obtain, transfer, deliver, or receive one or more credit card account numbers in any form

"(a) with the intent to defraud any consumer or other person; or

"(b) for any purpose other than a legitimate business purpose involving the credit card account or accounts, the cardholders, or the operation of the credit card system."

Sec. 2. Section 134 of the Truth in Lending Act (15 U.S.C. § 1644) is amended by redesignating the existing section as paragraph (a), by redesignating existing paragraphs (a), (b), (c), (d), (e) and (f) as paragraphs (1), (2), (3), (4), (5) and (6) and by adding a new paragraph (b) to read as follows:

"(b) As used in this section, the term "credit card" means a card, plate, coupon book, code, actual or fictitious account number, or other means of access, which if used alone or in conjunction with another credit card could permit a person to obtain credit or initiate an extension of credit. The aggregate one-year dollar values used in this section are to be calculated on the basis of the person or persons engaging in one or more transactions using one or more credit cards."

Sec. 3. The Electronic Fund Transfer Act (15 U.S.C. §§ 1693 et seq.) is amended by adding a new section to be designated section 922 to read as follows:

"Section 922. No person in a transaction affecting interstate or foreign commerce, or using any instrumentality of interstate or foreign commerce, shall sell, buy, furnish, exchange, obtain, transfer, deliver, or receive one or more account numbers in any form

"(a) with the intent to defraud any consumer or other person; or

"(b) for any purpose other than a legitimate business purpose involving the account or accounts, the account holders, or the operation of the debit account system."

Section 4. Section 916(c) of the Electronic Fund Transfer Act (15 U.S.C. § 1693n(c)) is amended to read as follows:

"(c) As used in this section, the term "debit instrument" means a card, plate, code, actual or fictitious account number, or other means of access (other than a check, draft, or similar paper instrument) which if used alone or in conjunction with another debit instrument would permit a person to initiate an electronic fund transfer, whether or not the account accessed by the transfer was established primarily for personal, family or household purposes. The aggregate one-year dollar values used in this section are to be calculated on the basis of the person or persons engaging in one or more transactions using one or more debit instruments."

Senator Hawkins. Thank you, Mr. Neumann.

Mr. Kelleher, we appreciate you traveling a long way for you to participate with us today. We have a copy of your full testimony and your summary. The danger in coming last is that a lot of it has been said. I wonder if you would be able to pick the high points out of your summary so we can ask questions.

STATEMENT OF THOMAS KELLEHER, VICE PRESIDENT FOR SECURITY, MASTERCARD INTERNATIONAL

Mr. Kelleher. Good morning. My name is Thomas F. Kelleher. Until 1982, I was the Assistant Director of the FBI Crime Laboratory and I spent 21 years with the FBI in several other capacities. I am now vice president, security of MasterCard International Inc. MasterCard International is a membership corporation composed of the over 13,000 U.S. financial institutions which issue and honor the familiar MasterCard credit and debit cards. MasterCard is extremely pleased to have the opportunity to come before this subcommittee today in order to help focus attention on the very real and growing problem of card-related fraud.

Historically, card-related fraud was a relatively contained activity, both in terms of the numbers of improper transactions and the dollar losses which resulted. Improper card use typically originated from a lost or stolen card which fell into the hands of an individual petty thief. In such case, the cardholder would miss his card and notify the card issuer of the unauthorized transaction promptly (usually no later than the next billing statement on which any unauthorized transaction(s) had appeared). The issuer could promptly block the card through the authorization system and publish the card account number as a restricted account which should not be honored further by banks or merchants. By blocking the account in the authorization system and by including an account as restricted, the issuer can provide an economic incentive to the merchant not to honor the account. The losses which resulted from these abuses typically occurred over a short timespan and were promptly brought to the attention of the card issuer for remedial action. Generally, too, these practices were perpetrated by an individual for his own personal gain, utilizing an actual plastic card initially issued as a valid, authorized card. Thus, the exposure from these frauds was of a limited nature.

FRAUD LOSSES GROW UNSPECTACULARLY

In 1973, total fraud losses for MasterCard members were $2,780,000. Over the course of the decade, fraud losses grew unspectacularly, keeping pace with the growth of transaction volume. However, beginning in 1980, the bank card industry began to experience an overwhelming and unexpected rise in the number and amount of card-related fraud as well as a change in the nature of this fraudulent activity. In 1979 total fraud losses for MasterCard members were $12,569,290. In 1980, MasterCard members reported $19,041,897 in fraud losses. For 1981, the figure was $25,817,918, a 36-percent increase. By 1982, losses escalated to $45,613,550, an increase over 1981 of $18.9 million or 77 percent.

Taken alone, the staggering increase in dollar losses is reason enough for concern. But, of at least equal concern is the type of activity responsible for the increase in these figures. Specifically, our research indicates that many of the card-related abuses which are reflected in the industry's losses today are of a type which were previously unimaginable and certainly not the "norm" when the existing card crime laws were enacted. Specifically, a new type of fraud has surfaced; fraud utilizing not the card itself, but the account number.

Offenders have devised several different ways to obtain valid account numbers without the cardholder knowing that the number will be used by another person. Account data can be extracted from carbon slips which were used in valid card transactions and either discarded by the merchant or memorized by the perpetrator while someone was making a legitimate purchase. Or, account data can be "conned" from the cardholder directly, generally over the telephone utilizing a variety of fraudulent techniques varying from purported surveying, to product offerings, to representations that the perpetrator is the bank confirming the account information. One practice of recent vintage involves collusion by a merchant or a merchant clerk who obtains valid account numbers taken from authorized sales at the merchant's place of business. These account numbers are transcribed onto sales slips which are then "sold" to other colluding merchants for deposit with their respective banks for payment. These latter merchants would enter such "phony" sales slips into the system commingled with valid slips so as to better conceal the scam.

Genuine account numbers are surely a valuable commodity. They can be used on unauthorized sales slips by dishonest merchants as described above, or, valid account numbers may be used to purchase goods from telephone/mail order houses. Goods would then be shipped to a temporary address given by the perpetrator who would change locations before the cardholder would report the unauthorized transaction from his billing statement.

More significantly, account numbers may also be used to create counterfeit cards. Card counterfeiting techniques have become distressingly popular among sophisticated criminals. One favorite method of counterfeiting employs a silk screening process (the same process used to print T-shirts). It is a common technique, inexpensive to use and has proven, unfortunately, to be an effective process. Briefly, a clear plastic card which can be obtained through many legitimate sources is silk screened with the design and registered service marks of a card organization. Then, valid account numbers obtained in one of the ways I just described, are embossed onto the card. The resulting product is a card that looks and acts, for a given period, as an authorized card. Another card fabrication scam utilizes a lost or stolen card. The criminal irons out the original cardholder identifying information on the card and re-embosses over it with different, valid account data. In 1982 our members reported that an estimated $9,337,354 were lost as a result of counterfeit card usage alone, an increase of 11 percent over 1980 and an unbelievable 769 percent over 1973 figures!

MasterCard estimates that the improper use of valid account numbers, whether through card theft for counterfeiting purposes or through collusive merchant activity, is largely responsible for the unprecedented increase in card fraud activity. Our research further indicates that the dramatiac increase in account number abuse is in large part the result of the participation and direction of sophisticated criminals, not the penny ante thief of earlier times.

ORGANIZED CRIME, VIOLENCE ASSOCIATED WITH ACCOUNT ABUSES

Most distressingly, organized crime figures prominently in the burgeoning card account abuses, as evidenced by recent arrests, investigations and newspaper reports. And, as is typically the case with organized crime, violence, prostitution and drug trafficking are associated with these activities. Postal Inspectors have arrested a number of people within the past 2 years who were allegedly associated with organized crime. In one case, two persons were arrested and charged with operating a counterfeit card ring. Shortly after their arrest, four men linked to them were found shot to death. The "street" rumor said that the dead men had "fingered" the two arrestees. In another case a man and his wife were arrested along with 6 other coconspirators and charged with 4 counts of conspiracy to commit credit card fraud. The couple were convicted and sent to Federal prison. The wife was paroled to care for her child. Eleven months after her arrest, the wife, her son, and her nephew, were slain gangland style in their home, while her husband was in jail. Thus, the nature of card-related abuses has changed from a nonviolent type of petty thievery involving isolated instances of dishonesty to a sophisticated, well-organized activity of far-reaching proportions that feeds into and supports the very worst elements of criminal society.

The compelling figures of the high cost of this crime clearly translate into higher dollar losses for card issuing institutions. For the record, we are submitting additional statistics and graphs evidencing the spiraling growth of this problem and indicating a likely upward trend. When industry is forced to absorb higher and higher costs for providing a service, those costs will, by necessity, be reflected in the price charged to consumers. Yet, it is not only in the price of services that consumers are impacted by this type of fraud. Consumers are also injured by the sheer annoyance of having to deal with improper charges on their account statements, of being forced to await a card replacement, of being conned over the phone and, generally, of being personally victimized by such abusive tactics. These latter injuries are hard to quantify, but easy to sympathize with.

Because we can not countenance the manipulation by others of the MasterCard service to harass consumers, and because of the costs we are forced to bear and pass on, the industry has not sat idly by watching this burgeoning activity. We at MasterCard have taken strong steps at many levels to stem the tide and to control fraud, beginning with the physical properties of the card itself. The MasterCard card has been redesigned to contain three anticounterfeiting features: fine line printing, ultra-violet ink printing, and a unique hologram covering part of the embossed account number. The hologram contains a laser produced three-dimensional image of the MasterCard logo. In addition to making the MasterCard card extremely difficult and costly to reproduce, it will make alteration of the embossed account number digits covered by the hologram much harder to accomplish and much easier to detect.

In our increasing awareness and horror at the rising tide of fraud, we have taken additional steps to control the abuse of account numbers by merchants. We have added a provision in the MasterCard Operating Rules which prohibits a merchant from providing, selling or exchanging account number information, in any medium, unless connected with the merchant's participation in the bankcard business.

These actions are only intended to exemplify the commitment of MasterCard to curtail these fraudulent practices and the whole of the bank card industry is working hard toward this end. But these continuing efforts are not enough. Congressional action is necessary to make changes in our current Federal laws affecting card activity. Specifically, the Truth-in-Lending Act, the Electronic Funds Transfer Act, and the existing card-related crime laws, do not adequately address the new types of criminal activity which have evolved since these laws were first enacted. These laws speak only in terms of abuse relating to the card itself. They do not reference at all abuse of the account number without the card. As you know, criminal statutes are strictly construed. Courts are hesitant to convict individuals where the language of the law cannot specifically by applied to the individual's actions. Consider, in this regard, the action of a Federal appeals court when presented with this very question as to whether misuse of account numbers was illegal under the Truth-in-Lending Act. The court held that the misuse of account numbers was not covered under the Truth-in-Lending Act since the scheme involved only account numbers and an actual card was not physically presented by the perpetrator. This is just the type of decision which frustrates law enforcement officials and makes them hesitate to pursue account-related abuses. It is also the type of decision which, we suggest, calls for a Congressional restatement of the card crime statutes.

LOOPHOLES IN EXISTING LEGISLATION

There are a number of other loopholes in the existing law which make prosecution of card crime difficult. One such loophole is that it is not a crime to counterfeit a card or to possess such a card in spite of the fact that cards provide the kind of exchange value offered by currency. Misuse of currency is, and should be, a crime of the highest priority. We submit that misuse of cards and account numbers should likewise be labeled as crimes and likewise be a priority.

There are several other deficiencies in the existing Federal law which we strongly suggest needs to be corrected. Whenever there are statutory deficiencies, technical barriers to prosecution are provided. It is therefore important for the card crime laws to be drawn as broadly as constitutionally permissible in order to provide prosecutors with the necessary tools with which to convict offenders. Attached to MasterCard's written testimony are copies of draft legislative changes to both title 15, the existing law, as well as to the general criminal code, title 18, which we feel are necessary to define the criminal nature of these activities and, thereby, assist in the prosecution of those persons involved.

In the evaluation and possible introduction of legislation, we wish to offer one cautionary note. While account numbers have been the subject of abuse by unscrupulous people, they are also essential to continuing legitimate business being transacted by banks, by MasterCard and by other legitimate organizations. Obviously, in order to transact MasterCard business, the merchants, the banks, MasterCard, and any of their agents, must be able to use the account numbers through the proper authorization, billing, collection, and other system activity. Account numbers are also provided as part of a bankcard portfolio sale or merger. Given the strict interpretation of the law, it is critical that any legislation which addresses the handling or distribution of account numbers must respect the needs of legitimate businesses to utilize those numbers.

Additionally, I'd like to add that I returned this moring from a meeting of the MasterCard Latin American Conference in Santiago, Chile, where I spent several days in conference with bank officials from Central and South America. Due to economic problems in several of these countries, the governments limit the use of credit cards to domestic activity alone.

Senator HAWKINS. Say that again. In Latin America they only let you use the card in their country?

Mr. KELLEHER. Yes; several of the countries in Latin America have limited, for economic reasons or for one reason or the other, the use of their credit cards for domestic use alone and in discussion with these bank leaders in South America a contributory factor listed was the fact that counterfeiting ran so high on Central and South American cards within the United States and many of these were obtained through the activities just recently described.

Without solid criminal statutes with which to prosecute offenders, it is apparent to us that industry efforts to control this problem will be undermined. Clearly, in the fight against such action, it is important for both industry and government law enforcement officials to be armed with a congressional directive that card account activities, as we have described, are a criminal affront against consumers, institutions, and society at large and shall not be tolerated.

On behalf of MasterCard International, I want to thank you for the opportunity to express our views. I will be pleased to answer any questions you might have.

[Complete statement follows:]

STATEMENT
OF
THOMAS F. KELLEHER
ON BEHALF OF
MASTERCARD INTERNATIONAL INCORPORATED
BEFORE THE COMMITTEE ON BANKING, HOUSING AND URBAN AFFAIRS
SUBCOMMITTEE ON CONSUMER AFFAIRS
UNITED STATES SENATE
MAY 18, 1983

Good morning. My name is Thomas F. Kelleher. Until 1982, I was the Assistant Director of the FBI Crime Laboratory and I spent 21 years with the FBI in several other capacities. I am now Vice President, Security of MasterCard International Incorporated. MasterCard International is a membership corporation composed of the over 13,000 U.S. financial institutions which issue and honor the familiar MasterCard credit and debit cards. MasterCard is extremely pleased to have the opportunity to come before this subcommittee today in order to help focus attention on the very real and growing problem of card-related fraud.

Historically, card-related fraud was a relatively contained activity, both in terms of the numbers of improper transactions and the dollar losses which resulted. Improper card use typically originated from a lost or stolen card which fell into the hands of an individual petty thief. In such case, the cardholder would miss his card and notify the card issuer of the unauthorized transaction promptly (usually no later than the next billing statement on which any unauthorized transaction(s) had appeared). The issuer could promptly block the card account through the authorization system and publish the card account number in our warning bulletin as a restricted account which should not be honored further by banks or merchants. By publishing an account as "restricted", the issuer can provide an economic incentive to the merchant to not honor the account. The losses which resulted from these abuses typically occurred over a short time span and were promptly brought to the attention of the card issuer for remedial action. Generally too, these practices were perpetrated by an individual for his own personal gain, utilizing an actual plastic card initially issued as a valid, authorized card. Thus, the exposure from these frauds was of a limited nature.

In 1973, total fraud losses for MasterCard members were $2,780,000. Over the course of the decade, fraud losses grew unspectacularly, keeping pace with the growth of transaction volume. However, beginning in 1980, the bank card industry began to experience an overwhelming and unexpected rise in the number and amount of card-related fraud as well as a change in the nature of this fraudulent activity. For the record, we are submitting additional statistics and graphs evidencing the growth of this problem and indicating its likely upward trend. Particularly noteworthy is the picture of fraud increase charted against transaction volume increase displayed in Appendix A. While the MasterCard system has enjoyed a steady increase in transaction volume the increase in fraud and counterfeit losses is dramatic and sudden. In 1981 our volume increased 232% over a base volume of 1973 and volume increased 255% in 1982. Fraud loss increases over 1973 losses for those years was 829% in 1981 and 1540% in 1982 respectively. Counterfeit losses increased an astounding 10,652% in 1981 over 1973 counterfeit losses and 76,763% in 1982! In 1979 total fraud losses for MasterCard members amounted to $12,569,290. In 1980, MasterCard members reported $19,041,897 in fraud losses. For 1981, the figure was $25,817,918, a 36% increase. By 1982, dollar losses escalated to $45,613,550, an increase over 1981 alone of $18.9 million or 77%!

Taken alone, the staggering increase in dollar losses is reason enough for concern. But, of at least equal concern is the type of activity responsible for the increase in these figures. Specifically, our research indicates that many of the card-related abuses which are reflected in the industry's losses today are of a type which were previously unimaginable and certainly not the "norm" when the existing card crime laws were enacted. Specifically, a new type of fraud has surfaced; fraud utilizing not the card itself but the account number.

Offenders have devised several different ways to obtain valid account numbers without the cardholder knowing that the number will be used by another person. Account data can be extracted from carbon slips which were used in valid card transactions and either discarded by the merchant or memorized by the perpetrator while someone was making a legitimate purchase. Or, account data can be obtained from the cardholder directly, generally over the telephone utilizing a variety of fraudulent techniques varying from purported surveying, to product offerings, to representations that the perpetrator is the bank confirming the account information.

Valid account numbers are surely a valuable commodity and have been used dishonestly in some unlikely ways. One practice of recent vintage involves collusion by a merchant or a merchant clerk who obtains valid account numbers taken from authorized sales at the merchant's place of business. These account numbers are transcribed onto sales slips which are then "sold" to other colluding merchants for deposit with their respective bank for payment. Or, account numbers can be used on "white plastic" cards. The white plastic fraud cases literally involve a card which does not bear any design or service mark on it. The card's face is embossed with a valid account number so that when presented to a dishonest merchant, the card can be imprinted on a sales slip and the slip could then pass as a valid transaction. Whether the slip is made by hand or against a white plastic card, these "phony" sales slips are entered into the system by the merchants, commingled with valid slips so as to better conceal the scam.

Account numbers can be used on unauthorized sales slips by dishonest merchants as described above or, used to purchase goods from telephone/mail order houses. Goods would then be shipped to a temporary address given by the perpetrator who would change locations before the cardholder would report the unauthorized transaction from his billing statement.

More significantly, account numbers may also be used to create a counterfeit card. Card counterfeiting techniques have become distressingly popular among sophisticated criminals. One favorite method of counterfeiting employs a silk screening process (the same process used to print T-shirts). It is a common technique, inexpensive to use and has proven, unfortunately, to be an effective process. Briefly, a plastic card which can be obtained through many legitimate sources is silk screened with the registered design and service marks of a card organization. Then, valid account numbers obtained in one of the ways I just described, are embossed onto the card. The resulting product is a card that looks and acts, for a given period, as an authorized card. Another card fabrication scam, not quite as sophisticated as card counterfeiting, utilizes a lost or stolen card. The criminal irons out the original cardholder identifying information on the card and re-embosses over it with different, valid account data obtained in one of the ways I just mentioned. One industry group has calculated that counterfeits comprise 14% of non-cardholder related fraud losses; account number alterations, 53%; white plastic, 22% and stolen blanks, 11%.

Based on our review of the fraud activity MasterCard estimates that the improper use of account numbers, whether through card alteration, card counterfeiting or through collusive merchant activity, is to a great degree responsible for the unprecedented increase in card fraud activity.

Our research further indicates that the dramatic increase in account number abuse, is in large part the result of the participation and direction of sophisticated criminals, not the penny ante thief of earlier times. For example, a school specializing in card fraud was recently uncovered in New Jersey. Students actually paid to matriculate in classes on counterfeiting and theft-related fraud. Upon graduation the students were sold cards to use. The alumni program provided the new graduates with a place to deposit stolen merchandise.

Most distressingly, organized crime figures prominently in the burgeoning card account abuses, as evidenced by recent arrests, investigations and newspaper reports. And, as is typically the case with organized crime, violence, prostitution and drug trafficking play a part of these activities. Postal

Inspectors have arrested a number of people within the past two years who were allegedly associated with organized crime. In one case two persons were arrested and charged with operating a counterfeit card ring. Shortly after their arrest, four men linked to them were found shot to death. The "street" rumor said that the dead men had "fingered" the two arrestees. In another case a man and his wife were arrested along with six other co-conspirators and charged with fourteen counts of conspiracy to commit credit card fraud. The couple was convicted and sent to federal prison. The wife was parolled to care for her child. Eleven months after her arrest, the wife, her son and her nephew, were slain gangland style in their home, while her husband was in jail. In New York City's Times Square area for example, a pool room served as a credit card supermarket. Card thieves, posing as prostitutes, would steal the cards from their clientele and then wholesale the stolen plastic at the pool room. Thus, the nature of card-related abuses has changed from a non-violent type of petty thievery involving isolated instances of dishonesty to a sophisticated, well organized activity of far reaching proportions that feeds into and supports the very worst elements of criminal society.

The compelling figures of the high cost of this crime clearly translate into higher dollar losses for card issuing institutions. Presently, we estimate that fraud losses cost the MasterCard system approximately $.08 per transaction, up from a cost of $.008

per transaction based on 1973 figures. This represents an increase in the cost of the MasterCard service of an overwhelming 900%. When industry is forced to absorb higher and higher costs for providing a service, those costs will, by necessity, be reflected in the price charged to consumers. Yet, it is not only in the price of services that consumers are impacted by this type of fraud. Consumers are also injured by the sheer annoyance of having to deal with improper charges on their account statements, of being forced to await a card replacement, of being conned over the phone and, generally, of being personally victimized by such abusive tactics. These latter injuries are hard to quantify, but easy to sympathize with.

Because we can not countenance the manipulation of the MasterCard service by others to harass consumers and because of the costs we are forced to bear and pass on, the industry has not sat idly by. We at MasterCard have taken strong steps at many levels to stem the tide and to control fraud, beginning with the physical properties of the card itself. The MasterCard card has been redesigned to contain three anti-counterfeiting features: fine line printing; ultra-violet ink printing and a unique hologram covering part of the embossed account number. The hologram contains a laser produced three-dimensional image of the MasterCard logo. In addition to making the MasterCard card extremely difficult and costly to reproduce, it will make alteration of the embossed account number digits covered by the hologram much harder to accomplish and much easier to detect. To further prevent transactions with fraudulent or altered cards, we have reprogrammed our authorization system to enable our members to better identify cardholders at the point of sale. However, some time will be required until the system is fully implemented and more time will be needed to measure its impact on this fraudulent activity.

In our increasing awareness and concern over the rising tide of fraud, we have taken additional steps to control the abuse of account numbers by merchants. We have added a provision in the MasterCard Operating Rules which prohibits a merchant from providing, selling or exchanging account number information, in any medium, to any other party unless connected with the merchant's legitimate bank card business.

We are actively cooperating and supporting local and federal law enforcement officials in the investigation and prosecution of card-related crimes. Each of our principal members has a security representative with whom we coordinate investigative activities and law enforcement assistance. This representation creates an important network of card security experts with which local officials can obtain support and assistance in investigating and prosecuting crimes. In this regard, MasterCard regularly maintains communication with these individuals when MasterCard is alerted to possible criminal activities in a given area in order to contain the spread of any criminal ring. And, as the national organization, we operate a computerized fraud reporting system to which all member institutions input information on fraudulent or questionable activity. MasterCard utilizes this system to monitor developments which on a local level may not of themselves indicate any reason for concern but which, on a national level, create a pattern of activity worthy of additional scrutiny and to assist in law enforcement efforts.

These actions are only intended to exemplify the commitment of MasterCard to curtail these fraudulent practices and the whole of the bank card industry is working hard toward this end, as well. We will continue to channel our energies and resources in this area but these continuing efforts are not enough. In our work with law enforcement agencies it became apparent that Congressional intervention is necessary. Federal prosecution of card abuse has been seriously hampered by the inadequacy of existing federal laws and it is industry's understanding that the criminal element in our society is well aware, and taking advantage, of the deficiencies in the law and the lower priority accorded to prosecution of these cases. Specifically, current federal laws affecting card activity, the Truth-in-Lending Act and Electronic Funds Transfer Act, do not adequately address the offenses which have evolved since these laws were first enacted. For example these laws speak only in terms of abuse relating to the card itself. They do not reference at all abuse of the account number without the card. As you know, criminal statutes are strictly construed. Courts are hesitant to convict individuals where the language of the law can not specifically be applied to the individual's actions. Consider, in this regard, the action of a court when presented with this very question as to whether misuse of account numbers was illegal under the Truth-In-Lending Act. The court held that the misuse of account numbers was not covered under the Truth-in-Lending Act since an actual card was not physically presented by the perpetrator although a valid account number, however, was presented.[1] This is just the type of decision which frustrates law enforcement officials and makes them hesitate before pursuing account-related abuses.

There are a number of other loopholes in the existing law which make prosecution of card crime difficult. One such loophole is that it is not a crime to counterfeit a card or even to possess such a card in spite of the fact that cards provide the kind of exchange value offered by currency. Misuse of currency is, and should be, a crime of the highest priority. We submit that misuse of cards and account numbers should likewise be labeled as crimes and likewise be a priority.

There are several other deficiencies in the existing federal law which we strongly suggest need to be corrected.

[1] United States v. Callihan, 666 F. 2d 422 (9th Cir. 1982)

Some of the subsections contain dollar amount minimums to trigger liability. There has been concern raised by law enforcement officials that these minimums technically must be applied to each card which is used, rather than each person or persons connected in a conspiratorial ring. An amendment to the law should be made to clarify that these dollar value tests are met by looking to one or more persons using one or more cards in one or more transactions. In this way, a person would not escape conviction if, for example, he used 100 different counterfeit cards to make purchases of $10,000, with each card responsible for only $100 of value.

Also, it is important that the recent experience with credit card fraud serve as a model for the debit card environment. Today, credit cards are commonplace whereas debit cards are not as numerous. Yet, the incidence of debit card customers is becoming much more frequent and will only grow larger. Therefore, it is important that the criminal laws relating to debit cards also be amended in order to reflect today's criminal devices and tomorrow's technology.

Whenever there are statutory deficiencies, technical barriers to prosecution are provided and criminals who might otherwise be convicted are released on "technicalities." It is therefore important for the card crime laws to be drawn as broadly as constitutionally permissible in order to provide prosecutors with the necessary tools with which to convict offenders. Attached in Appendix B are copies of a two step draft legislative approach which suggests changes to both Title 15, the existing law, as well as to the general criminal code, Title 18, which we feel are necessary to define the criminal nature of these activities and, thereby, better assist the prosecution of those persons involved. The Title 18 revisions we propose would specifically and comprehensively address criminal abuses of the credit card and debit card systems in a new Chapter dealing with these payment mechanisms. Among other things, our suggestions incorporate misuse of today's technology as well as that of tomorrow's. They combine the laws relating to credit and debit cards into one provision, much simpler to understand than existing law. However, while we believe these measures will prove helpful in the long run to reduce the alarming increase in card crime, immediate steps must be taken by this Subcommittee to plug the loopholes we described in the existing law that have developed as a result of the changing nature of card criminals. To that end, we have also suggested changes to Title 15.

In the evaluation and possible introduction of legislation, we wish to offer one cautionary note. While account numbers have been the subject of abuse by unscrupulous people, they are also essential to continuing legitimate business being transacted by merchants, by banks and by MasterCard and by other legitimate organizations. Obviously, in order to transact MasterCard business the merchants, the banks, and MasterCard, and any of their agents, must be able to utilize the account number.

Account numbers are transmitted in the authorization message and reply. Obviously, too, they appear in the records of the merchant, the merchant's bank, MasterCard and the card issuing bank. In the event of a dispute, account numbers are used to investigate a dispute among the parties enumerated above, or any of their successors or assigns. These numbers are also used in the collection process whether done in the institution or through a third party. Account numbers are also provided as part of a bankcard portfolio sale to or merger with another financial institution. Clearly, to be unable to provide the account number in this instance would not only drastically disturb the operations of the institutions involved but would also inconvenience the cardholder and would jeopardize the smooth continuation of the card service. In the event of a claim of counterfeit or fraudulent activity, the account number may be provided to an insurance company which may cover a portion of those losses. Similarly, in the event of any legal dispute for which insurance coverage may exist (e.g., credit slander) the account number will be provided to the carrier. And, of course, the account number must be provided to the card manufacturer so that an embossed card can be produced and provided to the cardholder. These instances are intended merely to illustrate the many and varied legitimate uses of which account numbers are made. In any legislative focus on this issue it would therefore be important to ensure that legitimate business is not hampered. And, in this regard it is important to emphasize that account number misuse is a criminal matter being perpetuated for unlawful purposes and gain by individuals organized to accomplish unlawful ends. It is not either the purpose nor result of the activities of legitimate businesses. Thus, it is critical that legitimate business use of account numbers not be painted with the same brush which properly taints criminal activity. Given the strict interpretation of the law, we suggest that any legislation in this area be written so as to prohibit those specific activities which are illegitimate for if written as a general prohibition with limited exceptions, one is sure to unintentionally embrace legitimate activities. It is critical that any such legislation respect the needs of legitimate businesses to utilize those numbers.

Without solid criminal statutes with which to prosecute offenders, it is apparent to us that industry efforts to control this problem will be undermined. Clearly, in the fight against such action, it is important for both industry and government law enforcement officials to be armed with a Congressional directive that card account activities, as we have described, are a criminal affront against consumers, institutions and society at large and shall not be tolerated.

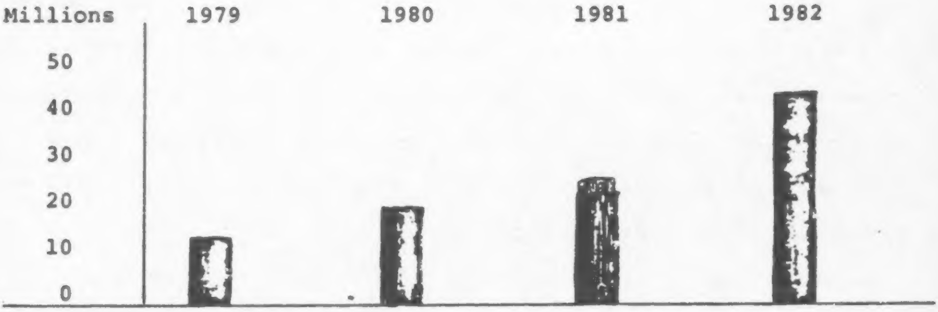
On behalf of MasterCard International, I want to thank you for the opportunity of expressing our views. I will be pleased to answer any questions you might have.

APPENDIX A

Fraud Losses Reported

1979	$ 12,569,290
1980	$ 19,041,897
1981	$ 25,817,918
1982	$ 45,613,550

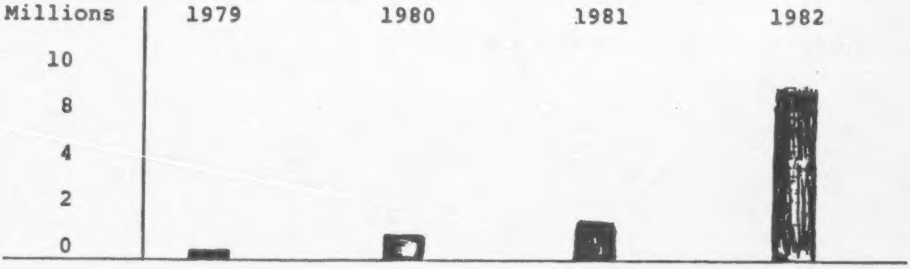
Illustration:

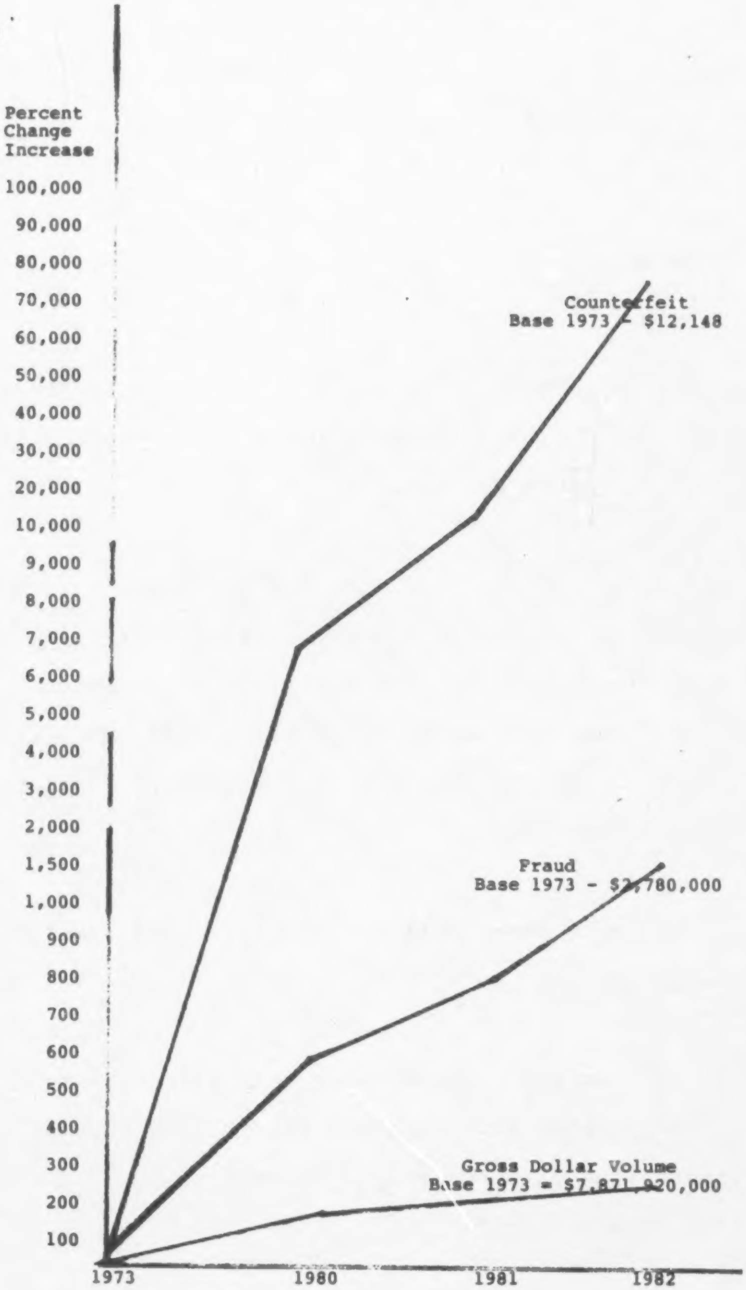


Counterfeit Losses Reported

1979	$ 172,143
1980	$ 839,379
1981	$ 1,306,148
1982	$ 9,337,354

Illustration:




Percent
Change
Increase
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
9,000
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,500
1,000
900
800
700
600
500
400
300
200
100
Counterfeit
Base 1973 - $12,148
Fraud
Base 1973 - $2,780,000
Gross Dollar Volume
Base 1973 = $7,871,920,000
1973
1980
1981
1982

APPENDIX B

DRAFT

[A bill to amend the Truth in Lending Act and the Electronic Fund Transfer Act.]

Sec. 1. The Truth in Lending Act (15 U.S.C. §§ 1601 et seq.) is amended by adding a new section to be designated section 129 to read as follows:

"Section 129. No person in a transaction affecting interstate or foreign commerce, or using any instrumentality of interstate or foreign commerce, shall buy, sell, furnish, exchange, obtain, transfer, deliver, or receive one or more credit card account numbers in any form

"(a) with the intent to defraud any consumer or other person; or

"(b) for any purpose other than a legitimate business purpose involving the credit card account or accounts, the cardholders, or the operation of the credit card system."

Sec. 2. Section 134 of the Truth in Lending Act (15 U.S.C. § 1644) is amended by redesignating the existing section as paragraph (a), by redesignating existing paragraphs (a), (b), (c), (d), (e) and (f) as paragraphs (1), (2), (3), (4), (5) and (6) and by adding a new paragraph (b) to read as follows:

> "(b) As used in this section, the term "credit card" means a card, plate, coupon book, code, actual or fictitious account number, or other means of access, which if used alone or in conjunction with another credit card would permit a person to obtain credit or initiate an extension of credit. The aggregate one-year dollar values used in this section are to be calculated on the basis of the person or persons engaging in one or more transactions using one or more credit cards."

Sec. 3. The Electronic Fund Transfer Act (15 U.S.C. §§ 1693 _et seq_.) is amended by adding a new section to be designated section 922 to read as follows:

> "Section 922. No person in a transaction affecting interstate or foreign commerce, or using any instrumentality of interstate or foreign commerce,

shall sell, buy, furnish, exchange, obtain, transfer, deliver, or receive one or more account numbers in any form

"(a) with the intent to defraud any consumer or other person; or

"(b) for any purpose other than a legitimate business purpose involving the account or accounts, the account holders, or the operation of the debit account system."

Section 4. Section 916(c) of the Electronic Fund Transfer Act (15 U.S.C. § 1693n(c)) is amended to read as follows:

"(c) As used in this section, the term "debit instrument" means a card, plate, code, actual or fictitious account number, or other means of access (other than a check, draft, or similar paper instrument) which if used alone or in conjunction with another debit instrument would permit a person to initiate an electronic fund transfer, whether or not the account accessed by the transfer was established primarily for personal, family or household purposes. The aggregate one-year dollar values used in this section are to be calculated on the basis of the person or persons engaging in one or more transactions using one or more debit instruments."

DRAFT

[To add a new Chapter to Title 18 to proscribe various activities in connection with payment devices.]

Chapter 76

Payment mechanisms

§ 1561 Definitions

As used in this chapter --

(1) "payment device" means any card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another payment device, to obtain money, goods, services, or any other thing of value, or to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2) "fraudulent payment device" means (A) any payment device or a facsimile, likeness, or similitude of a payment device that is counterfeit, fictitious, altered, forged, falsely made, lost, stolen, incomplete, expired, revoked, cancelled, fraudulently obtained, or obtained as part of a scheme to defraud, or (B) any invoice, voucher, sales draft, or other reflection or manifestation of such a device.

(3) "financial institution" means an institution with deposits or accounts insured by the Federal Deposit Insurance Corporation, the Federal Savings and Loan Insurance Corporation, or the National Credit Union Administration.

§ 1562 Fraud

(a) Whoever knowingly buys, receives, conceals, possesses, furnishes, exchanges, transfers, sells, delivers, or transports one or more fraudulent payment devices or any constituent part, component, or aspect thereof

(1) with unlawful or fraudulent intent;

(2) knowing the device to be a fraudulent payment device; and

(3) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using an instrumentality of interstate or foreign commerce, or (C) with a fraudulent payment device, or any constituent part, component, or aspect thereof, that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved 25 or

more fraudulent payment devices or constituent parts thereof, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(b) Whoever knowingly uses one or more fraudulent payment devices to obtain money, goods, services, or any other thing of value aggregating $1,000 or more in value in any one or more transactions occurring in any twelve-month period

(1) with unlawful or fraudulent intent;

(2) knowing the same to be a fraudulent payment device; and

(3) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using an instrumentality of interstate or foreign commerce, or (C) with a fraudulent payment device, or any constituent part, component, or aspect thereof, that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved money, goods, services, or any other thing of value aggregating $20,000 or more in value in any one or more transactions

occurring in any twelve-month period, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(c) Whoever knowingly buys, receives, conceals, possesses, furnishes, exchanges, transfers, sells, delivers, or transports money, goods, services, or any other thing of value aggregating $1,000 or more in any one or more transactions occurring in any twelve-month period

(1) with unlawful or fraudulent intent;

(2) knowing the same to have been obtained with one or more fraudulent payment devices; and

(3) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using an instrumentality of interstate or foreign commerce, or (C) with money, goods, services, or any other thing of value that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved money, goods, services, or any other thing of value aggregating $20,000 or more in any one or more transactions

occurring in any twelve-month period, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(d) Whoever knowingly buys, receives, conceals, possesses, furnishes, exchanges, uses, transfers, sells, delivers, or transports any actual or fictitious account information pertaining to a payment device or a fraudulent payment device, including without limitation account holders' names, account numbers, expiration dates, and identification or other access codes,

(1) with unlawful or fraudulent intent; and

(2) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) with respect to information that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved information pertaining to 25 or more payment devices, fraudulent payment devices, or accounts, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(e) Whoever attempts to commit, or solicits another to commit, any of the offenses described in this section shall be subject to the same penalty as attaches to the offense attempted or solicited.

§ 1563 Counterfeiting

(a) Whoever

(1) (A) falsely makes, forges, counterfeits, or alters any payment device or otherwise causes a payment device to become a fraudulent payment device, or (B) makes, devises, fabricates, or develops a fraudulent payment device, or any device or thing that can be used as, or in lieu of, a payment device, or that is or may be any constituent part, component or aspect thereof;

(2) with unlawful or fraudulent intent; and

(3) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) with a payment device, fraudulent payment device, device or thing that can be

used as, or in lieu of, a payment device, or any constituent part, component, or aspect of any of these that has moved in, has been part of, or constituted or with the intent that it will move in, will be part of, or constitute interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved 25 or more such devices or things, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(b) Whoever passes, utters, publishes, sells, brings into the United States, keeps in possession, or conceals any falsely made, forged, counterfeited, or altered payment device or any other fraudulent payment device or any constituent part, component, or aspect thereof,

(1) with unlawful or fraudulent intent; and

(2) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) with any such payment device, fraudulent payment device, or any constituent part, component, or aspect thereof that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved 25 or more fraudulent payment devices or constituent parts thereof, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(c) Whoever buys, sells, uses, exchanges, transfers, receives, or delivers any falsely made, forged, counterfeited, or altered payment device or any other fraudulent payment device or constituent part, component, or aspect thereof,

(1) with the unlawful or fraudulent intent that the same be passed, published, or used as true and genuine; and

(2) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) with any such payment device, fraudulent payment device, or any constituent part, component, or aspect thereof that has moved in, has been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than ten years, or both; and if the violation involved 25 or

more fraudulent payment devices or constituent parts thereof, shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(d) Whoever, with unlawful or fraudulent intent, obtains control, custody, or possession of any equipment or mechanisms used or that can be used to make, devise, fabricate, or develop fraudulent payment devices or any constituent part, component, or aspect of a device or thing that becomes or can be used as, or in lieu of, a payment device,

(1) by making, devising, fabricating, or developing a fraudulent payment device including any constituent part, component, or aspect of a device or thing that can be used as, or in lieu of, a payment device; and

(2) does so (A) in a transaction affecting a financial institution or interstate or foreign commerce, (B) using any instrumentality of interstate or foreign commerce, or (C) using such equipment or mechanisms that have moved in, been part of, or constituted interstate or foreign commerce;

shall be fined not more than $10,000 or imprisoned not more than fifteen years, or both.

(e) Whoever attempts to commit, or solicits another to commit, any of the offenses described in this section shall be subject to the same penalty as attaches to the offense attempted or solicited.

§ 1564 Presumption

For purposes of this chapter, the possession of eight or more fraudulent payment devices or of account or other information pertaining to eight or more fraudulent payment devices shall create a presumption that unlawful or fraudulent intent existed with respect to a specified act or activity, but such presumption shall be rebuttable.

§ 1565 Application for a payment device*

Whoever knowingly makes any false statement or report, or willfully overvalues any land, property or security, for the purpose of influencing in any way the action of any person (1) that moves or engages in interstate or foreign commerce or whose transactions in this regard affect interstate or foreign commerce and (2) that offers or issues payment devices, upon any application, advance, withdrawal, discount, purchase, purchase agreement, repurchase agreement, invoice, voucher, sales draft, commitment, or loan, or any change or extension of any of the same, by renewal, deferment of action or otherwise, or the acceptance, release, or substitution of security therefor, shall be fined not more than $5,000 or imprisoned not more than two years, or both.

---

* A preferable alternative to including this provision as a separate section here might very well be to add it as a new subsection (b) to existing 18 U.S.C. § 1014, which this section follows very closely.

§ 1566 Repeated violations

Whoever engages in any activity proscribed in sections 1562 or 1563 after one or more prior convictions for him under either of these sections have become final shall be fined not more than $20,000 or imprisoned not more than 20 years, or both.

Senator **HAWKINS**. Thank you.

Senator D'Amato, do you have any questions?

Senator **D'AMATO**. Thank you very much.

RESEARCH FOR COUNTERFEIT-PROOF CREDIT CARD

What about the possibility of coming up with a credit card that is counterfeit-proof or doing as much as can be done in that regard. Without mentioning the names of various types of cards, testimony thus far reveals that there obviously are distinctions. What is the industry prepared to do? It is one thing to say that we need stricter Federal legislation, that we need better enforcement—and I agree that we do need that—but also I think, as you indicated, there has to be and should be complementary industry efforts to assist law enforcement practices that are implementing authorities in curbing this activity. What can be done in this regard from the industry perspective?

Mr. **KELLEHER**. Senator, under the recent guidance of the American Bankers Association Task Force on Fraud, both VISA and MasterCard have contributed to a research project to come up with credit card properties that might be used in the manual mode. As quickly as possible, as these features have been identified and found workable, they are being implemented by our company. The limiting factor being that they have to be feasible economically since we can't burden the consumer with the losses.

Senator D'AMATO. Let us get right to the point. What are we talking about in increased costs? What range are we working in and what is feasible in terms of increased costs to the consumer? Mr. Neumann, have you been involved in calculating these figures?

Mr. NEUMANN. Yes; VISA has done extensive research independently as well as working with the American Bankers Association. I might point out that there is no such thing as a card that cannot be replicated in a form that could probably be passed in counterfeited circumstances. Therefore, we want to put those properties into cards that can be a major deterrent to the counterfeiters and make it more difficult for them to alter cards. The industry is expending a lot of money on research to come up with different devices and the cost is going to run anywhere from a few pennies a card to maybe 40 or 60 cents, depending on which ones are incorporated.

Senator D'AMATO. Now, let's look at that. Perhaps one of the reasons that we haven't made more progress in curbing credit card counterfeiting and the unauthorized use of credit card numbers is due to the over-aggressive marketing of the cards. You know, I get these cards mailed to me and, often, I throw them out. Recently, I was not informed that my office manager had ordered me one of these cards and I received it in the mail and I bent it and threw it out. Finally she said to me, "Senator, did you get your card?" And I said, "No." She said, "They told me they sent it to you." It had indeed been sent to me.

My point is, though, that that is the only one time I ever ordered a card yet I get all types from the local stores without even having to sign anything.

Senator HAWKINS. Now, you're supposed to sign. It's the law that you sign them.

Mr. NEUMANN. I think, Senator, there is a Federal law requiring that it be signed.

Senator D'AMATO. I guess you have to sign before they can foward a card to you. But you couldn't use such liberal merchandising techniques if the cost of the card were let's say maybe $1.

Mr. KELLEHER. Senator, could I add one thing?

Senator D'AMATO. Please, I want to finish this point.

What if the cost was $1 per card? Would that be a terribly burdensome cost to the consumer? In other words, if you could develop a card which was fairly hard to duplicate, would the cost be prohibitive to your customers?

Mr. NEUMANN. While $1 does not sound like much, the realities of the situation are that VISA alone has about 90 million cards that are in circulation worldwide at the present time; so the cost when viewed in the aggregate is significant. In addition, it's a slow process to replace these cards, so we're still looking down the road a few years before we can get a real stable secure card in place.

Senator D'AMATO. All right. But we admit that there is some consensus that the industry is not making its best efforts in developing the kind of card that would pose substantial problems for a counterfeiter.

Can any of you give us an estimate as to what overall credit card fraud losses would be if we were to take into account losses incurred by private label bank cards, retail cards, gasoline cards, travel, and entertainment cards. Has any body ever investigated that? Because I think were really talking into the hundreds and hundreds of millions of dollars here for overall industry losses.

Mr. **Neumann**. We're talking about $1 billion a year for the entire credit card industry.

Senator **D'Amato**. A billion dollars a year?

Mr. **Neumann**. Yes; but I'd like to add that the industry is really cleaning up its act. Both MasterCard and VISA as well as American Express have put a lot of money into establishing a good security type service. We're coming up with fraud reporting systems, working with law enforcement and taking the necessary steps to do our part in the industry, but we also need legislation.

Senator **D'Amato**. I think you sense from both the chairman's comments and from mine that we are rather sympathetic of the industry's problems in this area. We are also strongly supportive of corrective legislative efforts and increased law enforcement efforts in this area before it is allowed to continue to escalate in the geometric proportions it has in recent years.

Alice Skaggs of the Consumer Affairs Office in West Palm Beach, she probably lived in New York before coming down to Palm Beach——

Senator **Hawkins**. She did.

Senator **D'Amato**. You're taking all my good people, Paula.

USING CARBONLESS COPIES OF CREDIT CARD SLIPS

Senator **Hawkins**. That's right. Alice Skaggs of the Consumer Affairs Office in West Palm Beach, Fla., has strongly recommended that all credit card charges be made on carbonless paper in order to eliminate the element of credit card fraud that relies on retrieving carbon copies of credit card slips. Do you agree with this recommendation. Is the industry moving in that direction? If so, how rapidly? If not, why? This method is supposedly more expensive to the industry.

Mr. **Alexander**. Senator, we are moving in that direction. There really are two sales draft types available in the marketplace right now. One is the carbonless draft you referred to.

Senator **Hawkins**. Does American Express use that?

Mr. **Alexander**. I do not know, Senator. I think they are in pilot tests today. There's also a draft similar to the one you and I would have used for years that has a perforation in the carbon and after it's been torn apart the carbon is actually separated in the middle of the account number and it's much more difficult to match up account numbers. That adds more cost to the merchant and the merchants' banks. The carbonless draft, I personally have heard numbers from 5 to 50 cents per card. I can't be specific here today.

Mr. **Kelleher**. We're field testing now in many areas and we will be following that.

Senator **Hawkins**. To follow up on that, isn't it costing the consumers a lot the way it is today? The consumers are paying all of these losses, right? So when you say it's going to cost a dollar for any kind of card which may not be acceptable or that NCR paper is too expensive maybe, I think maybe you're looking at it from the wrong angle. I think it's very expensive not to do those things immediately and especially if you put out on the television with the 90 million you said are VISA holders it's just going to take a long time to get a card that will be counterfeit-proof or safer. There's nothing counterfeit-proof, but safer. It seems to me you're almost giving us a signal saying to hurry up and use them.

Mr. **NEUMANN**. That is one part of the problem, Senator, but they're getting the account numbers, unfortunately, from other sources than the carbons, particularly the organized criminal groups that buy these numbers illegally. This is a separate problem.

Mr. **KELLEHER**. I'd like to say that we are adopting new methods in credit card manufacturing. As a result of the ABA task force we have identified three things that could be used to keep people from counterfeiting cards with these simplistic methods, and that is to adopt fine-line printing, to use ultraviolet sensitive inks and to adopt a hologram which is one of those exciting things that comes along once in a while technically which provides the state of the art use of a three dimensional image on the card that to date can only be done by one or two highly sophisticated manufacturers. And we feel in that sense we have cost effectiveness right now at 2.5 cents each for holograms and probably no change in the cost to add fine-line printing and ultraviolet inks. They have been incorporated in the new MasterCard that's currently being issued. So we have adopted these and that's in the manual mode being used today.

There are two ways in which transactions take place. One in the manual mode and one where electronics are involved in the electronic point of sale. We have to adopt now what we can in the manual mode and we have been doing that as rapidly as possible. We are researching and improving our techniques and capabilities for the electronic mode as it comes along.

So it's a case of getting it out now while it's still useful and we're attempting to do that as rapidly as possible with the new card.

Senator **D'AMATO**. I have no further questions. I would ask one thing, though. In terms of your legislative proposals, you might best serve your interests if you were to have some of your legal people meet with some of our staffers to review your proposals and also to respond to some of the objections that you heard posed by the Justice Department and the Postal Service to those proposals. I think we might be able to begin to narrow some of those differences and come up with some legislation that everybody agrees on. That is a much easier process than fighting the administration.

Senator **HAWKINS**. This same Mrs. Skaggs who's very famous in Florida said she could not come today, I showed her testimony earlier—this is her testimony—she had an accident and could not come, but she's a very valid resource because she's the head of the Consumer Affairs Office in Palm Beach. In her written testimony she recommends that the sale or dissemination of such lists with account numbers be outlawed.

SALES OF LISTS WITH ACCOUNT NUMBERS

It would appear that such a prohibition would protect both the banks and the card holders and yet I understand the banks have a problem with that. Is that true or do you support the outlawing of the sale of lists with account numbers?

Mr. **Alexander**. I think first of all, Senator, most banks don't sell their lists of credit cardholders and when they do it's prudently done, but beyond that ——

Senator **Hawkins**. What is prudently? What does that mean?

Mr. **Alexander**. Well, where the bank knows exactly the use that will be made of it, what service will be merchandised or sold to those customers of the bank. They know the merchant with whom they're dealing, the purpose to which this will be put, and no other use will be made of it.

Senator **Hawkins**. Do you have a contract?

Mr. **Alexander**. As a general rule. I don't have any personal experience with that, but as a general rule, I believe they do, yes. More importantly, our concern is that we look to legislate against the disclosure of account numbers where there's an intent to defraud. If a bank employee discloses an account number with an intent to commit a fraud or to assist in committing a fraud, that that be strongly legislated against, as opposed to broad proscriptions against the dissemination of account numbers where we then have to write numerous exceptions which say you can do it here and you can do it here but you can't do it here and here, and we have regulation and we have compliance and we're petitioning then for exceptions. We would rather see it approached from the standpoint of if it's disclosed with the intent to commit a crime.

Senator **Hawkins**. Do the banks give out the bank account numbers of their customers, not the credit card numbers? Do you disclose or sell the bank number?

Mr. **Alexander**. Not to my knowledge, no.

Senator **Hawkins**. What is the difference in distributing or selling a credit card number list to someone? Aren't you protecting the privacy of your customer account by not giving out the account number of your customers?

Mr. **Branam**. Senator, if I may answer that, I don't think any banks are actually in the process of selling account numbers. What occurs is that many times a cardholder will sign up for an insurance program and the insurance program will require a billing of the account holder's card account. Therefore, the insurance company needs the account number to handle electronic billing process. Account numbers are given to the credit bureaus and that's proprietary information. They need the account number so they can properly identify the account in the bureau and make sure it's the same person that has that account.

There are other reasons for passing account numbers in the system which include authorizations which include giving information to collection agencies. There are several uses, but I don't think that the banks are ever indiscriminately passing out account numbers and if there is any arrangement, say, with an insurance company, that's always contractual.

Senator **Hawkins**. Well, one last statement before I dismiss this panel. Senator D'Amato indicated he had a problem with someone calling and ordering a limousine for him and charging it to his credit card number. In your new manual of instructions to those using these cards, why don't you require verification by telephone?

Did you really call? Even our local pizza parlor will call you and verify that someone called and ordered a pizza delivered to your house and before they deliver the pizza they'd like to know if you really want it. You have to give a phone number now when you order a pizza. That's such a fun thing to do to people. So it seems to me that we were talking about maybe they wouldn't have sent a limousine and maybe they shouldn't charge for items to someone that might be on their hit list. What's wrong with putting in your operations manual on that any telephone solicitations you call that person back?

Mr. Neumann. Senator, there may be a problem with respect to privacy. If a merchant, who receives a telephone order, calls the issuing bank to get information to verify that that it is in fact the account holder, the issuring bank may be precluded from providing the information under the financial privacy laws.

Senator Hawkins. But they can send a car?

Mr. Neumann. No; what I'm saying is that in many instances the bank cannot give that information out. Very often the merchant will try to get a number and call back in order to verify the transaction.

Senator Hawkins. In this instance, the bank wouldn't be involved. It would be up to the limousine service owner before he bills Senator D'Amato and asks him if he really wants this pizza.

Mr. Neumann. If he has Senator D'Amato's home telephone number and address. That would be up to the issuing bank to make that——

Senator Hawkins. Where is he delivering the limousine? I was talking about that one instance. Obviously they ordered the limousine and they were going to send it. There's only one Senator D'Amato, let me testify to that.

Mr. Kelleher. What we can do is set up rules by which accounts or transactions can be charged back when not authorized and just train the merchant base that should they choose to go outside of these procedures, they do so at their own risk. And in that sense, if there were excessive charge-backs over a period of time, this would be considered a problem and more than likely the bank that's handling the merchant would at that time review the account. In effect, the merchant is stepping outside the regulations that exist within the manual and our disciplining amounts to just having him cease and desist these dealings within our organization. But there is relatively little we can do beyond that.

Senator Hawkins. What about these internal abuses within the banks? We've got a lot of figures in tons of material. We will need to draft the new legislation. What amount of fraud is internal by your own employees charging things to an account that does not get the service?

Mr. Alexander. Those situations have occurred, Senator, just as the Postal Service indicated earlier.

Senator Hawkins. Yes, they gave testimony on that, but I understand it's in monumental proportions in Florida right now, internal fraud.

Mr. Branam. I don't know if it's monumental proportions. There have been some isolated instances that I'm aware of. But it's much easier controlled within the bank than it is outside because we have within our computer system certain secure methods to keep the information from going out.

Senator Hawkins. Thank you, gentlemen, for your participation today.

We will now call our last panel consisting of Milton Schober, Walter Kurth, John Baker, and William Price.

Mr. Schober, we'll call on you first on behalf of the American Retail Federation.

STATEMENT OF MILTON SCHOBER, ESQ., ON BEHALF OF AMERICAN RETAIL FEDERATION

Mr. Schober. Madam Chairman, I would submit our statement in full and ask that it be included in the record of these hearings. I will summarize that already brief statement for the purpose of oral presentation. As you stated, I am Milton Schober. I'm here today on behalf of the American Retail Federation.

I think it's only fair to state right at the outset that this Nation's merchants are in favor of fraud prevention and in principle they support the proposition that every legitimate measure should be taken to help stamp out fraudulent credit card practices.

However, there are a number of statutes already on the books that deal with certain aspects of fraud control. ARF urges caution therefore in this legislation so that the matter of fraud prevention does not become a patchwork of legislative overlapping and partially conflicting statutes that exists in so many other areas, particularly in the consumer credit protection field.

URGE CAUTION IN APPROACHING LEGISLATION

We also urge caution in approaching legislation such as this because it must be very carefully crafted in order not to discourage legitimate innovation in message delivery and authorization systems, and in joint ventures that are now being put together to deliver goods and services to the consuming public.

One of the main concerns that we have with the hearings today is that there is no Senate bill in front of us for America's merchants to examine and upon which to offer specific comments and views. The American Retail Federation urges the subcommittee to conduct additional hearings once a bill has been introduced and the interested parties have had an opportunity to examine it, and to offer further views on it, because we believe that the legislative process is vastly improved by the interested public's having had the opportunity to review legislation and to offer specific comments.

Another concern of ours is that any such legislation address specific abuses. For example, we feel that any legislation should identify with particularity any parties that are covered by it and any activities that are prohibited or otherwise limited so that we don't wake up one morning in the middle of what we think to be a legitimate undertaking and find that what we're doing may be against the law. We believe that the definitional sections of any statute should be drawn with particular care.

Similarly, we believe that it should avoid overlap with existing statutes. By way of example, we believe that the existing provisions of the Fair Credit Billing Act adequately protect the consumers against erroneous and unauthorized charges and we would urge the Congress not to replicate these provisions in additional legislation.

Finally, we urge the Congress to be aware that there are legitimate uses of lists. For example, any legislation specifically should permit intra company exchanges of lists. Many merchants are in fact multicorporate families that are incorporated in several jurisdictions for purposes of management or for purposes of chartering or for any number of internal reasons. But they are, in fact a single corporate family, and they function as a single corporate family. We would oppose vigorously any legislation that would prohibit the passing of customer lists between members of the same corporate family.

Similarly, lists have legitimate places in marketing activities in this day and age. For example, a merchant that honors a third party card may very well want to announce a special merchandise sale to the persons who hold that card in his trade area and any legislation should permit that customer to make a mailing to those persons if the customer can work it out with the bank or with the card exchange that issues the card and has the list.

By way of footnote, I see personally no reason for the numbers of the cards to be disclosed in that instance, but certainly it is an illustration of one of the problems that merchants face unless this legislation is very carefully drawn.

HOT CARD LISTS

Legislation should also avoid preventing the use of hot card lists. Hot card lists identify cards that should not be honored. I'm sure you've been in a store and used your card and they will pull out a little book with nothing but numbers in it. The card holder is not identified, but the use of those lists is absolutely necessary to prevent further losses both to financial institutions and to the merchants who honor the cards.

Finally, the retail industry's concern is that any legislation provide real protection against fraud for the parties involved that suffer the loss. For example, under many dealer agreements today between bank cards and merchants, when a merchant honors a fraudulently used card number, and the card holder properly claims a billing error under the Fair Credit Billing Act, the card issuer has the right to charge the merchant for the loss. Now this characteristically happens in a mail order or telephone order situation where the order is called in and there is no way for the person calling it in to be identified. The merchant that honored the card number must then eat the loss.

In this connection I understand that the National Retail Merchants Association, which is one of the American Retail Federation's constituent national trade association members, is in the process of gathering data on the magnitude of credit card loss problems in the retail industry. I heard that question a little while ago, how much would it be overall. In understand that NRMA will share the results of its data collection efforts with the Subcommittee.

On behalf of ARF, I thank you for this opportunity to summarize our views. I will be delighted to answer any questions I can: If I cannot, I'll supply written answers for the record.

[Complete statement follows:]

STATEMENT OF
MILTON W. SCHOBER
REPRESENTING THE
AMERICAN RETAIL FEDERATION

Madam Chairman, and members of the Subcommittee on Consumer Affairs, I am Milton W. Schober, and I am appearing today on behalf of the American Retail Federation (ARF) in my capacity as special credit counsel to the Federation.

Membership in ARF is composed primarily of state and national retail trade associations which, through their members, represent more than one million retail establishments.

Most retailers represented through ARF offer or extend consumer credit in some form. Many of them offer their own credit card plans; others honor three-party credit cards, such as Visa, Mastercard, and American Express; and others honor both their own cards and three-party cards. Many of them also utilize various lists from time to time for legitimate marketing and fraud control purposes. Thus, ARF is vitally interested in any proposal that Congress consider adopting more stringent rules to contain credit card fraud.

Obviously, this Nation's merchants are in favor of fraud prevention and, in principle, they support the proposition that every legitimate effort should be made to stamp out illegal credit card practices. However, a number of statutes already are on the books that deal with certain aspects of fraud control, and ARF urges caution in approaching the subject so that the matter of credit card fraud prevention does not become a patchwork of overlapping and partially conflicting laws that are extremely difficult to interpret and apply. Unfortunately, many other areas in the spectrum of consumer credit protection have a history of patchwork treatment with the result that it is an extremely complex area of the law that is difficult for both creditors and consumers to understand.

ARF also urges caution in approaching legislation such as this, because it must be carefully crafted in order not to discourage legitimate innovation in message delivery and authorization systems now coming on the market.

One of the retail industry's main concerns this morning is that there is no Senate bill to examine and upon which to offer specific views and comments. Obviously, the Subcommittee needs to know the magnitude of the problem before it finally approves legislation, and ARF endorses the Subcommittee's efforts in trying to determine that magnitude through these hearings; however, the Federation urges the Subcommittee to conduct additional hearings after a bill has been introduced and all interested parties have had the opportunity to examine it. The legislative process is vastly improved when interested parties are given the opportunity to comment on specific legislative proposals and work with the Congress in fashioning legislation that accomplishes its purpose without restricting legitimate activities.

Another industry concern is that any legislation should address the specific abuses found to exist and should do so in very precise terms. For example, identification of parties covered by the legislation and definitions of proscribed activities should be made crystal clear so that neither consumers nor creditors are inadvertently prohibited from legitimately using credit cards, or credit card numbers or other access information, or lists of credit card customers.

Similarly, ARF urges that any such legislation avoid duplication and overlap with existing statutes. Again, by way of example, ARF believes that the current Fair Credit Billing provisions of the Truth in Lending Act deal adequately with protecting consumers against erroneous and unauthorized charges. The retail industry urges the Congress not to replicate these provisions in other legislation dealing with the same subject.

ARF also is concerned that any such legislation recognize that legitimate uses are, in fact, made of credit card lists. For example, any such legislation specifically should permit intra-company use of account information, such as between subsidiaries of the same parent or between parent and subsidiary. Many multi-corporate entities are so organized for management purposes or because of chartering considerations, even though they function as a single entity. All information, including information about credit card customers, should be able to pass freely among all members of the corporate family.

Similarly, solicitation lists have a legitimate place in today's marketing activities. For example, a merchant honoring a given three-party credit card quite legitimately may want to advertise a special merchandise sale to the holders of that card in its marketing area. No legislation should prevent a retailer from mailing a promotional piece to the holders of the card that it honors. After all, those cardholders have an interest in knowing when sale merchandise is available.

Legislation also should be careful to avoid proscription of "hot card lists." These are lists of the numbers of accounts with no "open to buy"; that is, accounts to which additional charges are not authorized. An account number may appear on such a list for a variety of reasons, such as the card's having been reported lost or stolen, or the account's having become delinquent, or an authorized user having been taken off of the account by the accountholder. Whatever the reason, losses would escalate and commerce would suffer if such lists were proscribed.

Finally, the retail industry's concern is that any such legislation provide real protection against fraud for the parties involved that suffer the loss. For example, under many dealer agreements today, when a merchant honors a fraudulently used credit card number and the cardholder properly claims a billing error under the Fair Credit Billing Act, the card issuer has the right to charge the merchant for the loss, notwithstanding the fact that the merchant has followed established authorization procedures. This occurs when the name and account number of a valid account are used in a mail or telephone order or under similar circumstances in which the person presenting the name and account number cannot be identified. The merchant honors the number, but the cardholder refuses to pay, and it is the merchant who is stuck. Any legislation should seek to protect the injured party -- in this case, the merchant.

I understand that the National Retail Merchants Association (NRMA), one of ARF's constituent national trade association members, is gathering data on the magnitude of the credit card fraud problem among retailers. I also understand that NRMA is planning to present its findings to the Subcommittee for the record in these hearings as soon as the data have been tabulated and compiled.

On behalf of ARF, I thank the Subcommittee for this opportunity to present an overview of retail industry views on credit card fraud and the use of cardholder lists. The Federation will be in a position to offer more specific comments after a Senate bill has been introduced.

I will be delighted to attempt to answer any questions the Subcommittee may have, and if I am not able to do so today, I will supply them in writing for the record.

Senator HAWKINS. Thank you. The Senators who had to leave for other committee hearings may have other questions. We will leave the record open for a period of time.

The next witness will be Mr. Walter Kurth, president, Associated Credit Bureaus in Houston, Texas.

STATEMENT OF WALTER R. KURTH, PRESIDENT, ASSOCIATED CREDIT BUREAUS, HOUSTON, TEX.

Mr. KURTH. Thank you, Madam Chairman. My name is Walter Kurth and I'm president of the Associated Credit Bureaus which is an international association that was founded in 1906 to represent the consumer credit reporting industry.

Accompanying me today on my immediate left is John Baker, president and treasurer of the Credit Bureau of Georgia; and on my far right, William B. Price, president of CBC Companies in Columbus, Ohio.

With your permission, we'd like to submit our statement for the record and merely summarize in our oral remarks.

[Complete statement follows:]

STATEMENT BY WALTER R. KURTH

Madam Chairman and Members of the Subcommittee on Consumer Affairs of the Senate Committee on Banking, Housing and Urban Affairs, my name is Walter R. Kurth. I am president of Associated Credit Bureaus, Inc. (ACB). ACB is an international trade association founded in 1906 to represent the consumer credit reporting industry. Accompanying me today are John Baker, president of CBI, Atlanta, Georgia, and William B. Price, President of CBC Companies, Columbus, Ohio.

We appreciate the opportunity to appear before you to discuss the role of credit card account numbers in consumer credit reporting. Our testimony will be given in three parts. I will outline the scope of the industry and in general terms how the industry operates. Mr. Baker and Mr. Price will then discuss their own specific operations.

For the most part, credit bureaus or credit reporting agencies are sole proprietorships, partnerships or corporations. Approximately 420 members of our association operate from computer files while 1,250 are manual operations. The credit reporting industry produces, by conservative estimate, 200 million credit reports annually.

By way of definition, a credit bureau is a clearinghouse of information identifying the paying habits of consumers. Credit reporting files include identifying information such as name, spouse's name, address and former address, employer and former employer, social security number and number of dependents. Much of this information is supplied by the consumer when applying for credit.

Each month local, regional and national credit grantors send information on their customers to the credit reporting companies. This information shows how much is owed, whether the customer is current in his or her payments and how many times, if ever, the customer has been behind in his or her payments during the past 12 to 24 months. Most of these users are either retailers, banks, finance companies, mortgage lenders, oil companies or other credit card issuers.

Public record information on consumers is also filed.

All of the items I have identified come together to form a solid base of information in order that prudent credit granting decisions may be made. The keystone to the system is the manner in which the information is matched with the proper record.

We estimate the credit reporting industry receives in excess of 550 million lines of trade per month. As you can see, that kind of volume necessitates the use of positive identifiers to insure that information and consumers are properly matched. The primary identifier to achieve a successful match is the consumer's account number. For this reason it is essential that the account number is included when a credit grantor furnishes information.

With the advent of automation, credit grantors have for many years been asking consumers that account numbers of credit references be given on credit applications. This assures the consumer that the credit bureau or the credit grantor will in fact be able to locate the account on which the consumer was depending as a valuable credit reference. Without the account number, consumers were sometimes frustrated when credit grantors were unable to locate the reference account.

Account numbers also appear on the actual credit report. There are essentially two reasons for this. First, the number serves as an identifier linking the consumer and the account. This is true not only when the report is purchased for use by a credit grantor, and matched against the credit application, but also in a file disclosure situation where the consumer is made aware of the contents of his or her file. The presence of the account number is an assurance to the consumer that the payment history information is properly linked. Second, a credit grantor that desires more up-to-date information than that contained in the report may use the account number to check directly with the consumer's creditors before making a credit granting decision.

Credit card account numbering systems have greatly facilitated the exchange of commerce. Unfortunately, society will always have a few unscrupulous individuals who will attempt to use any system or procedure for their own dishonest gain.

While credit bureaus have strict safeguards to prevent misuse of credit card account numbers, there is no lack of ingenuity on the part of those who might attempt to circumvent those safeguards. It was in recognition of this fact that Congress included in the Fair Credit Reporting Act Section 619, providing for fine or imprisonment for obtaining credit bureau information under false pretenses.

For those who want to abuse the system, credit card account numbers can be easily obtained from many other sources and put to fraudulent uses. For example, some companies request the consumer to put an account number on the back of the payment envelope to facilitate mail sorting. Also, cards are often out of sight of the credit card holder during a credit transaction. For example, restaurants or self-service gas stations that require payment in advance. Card invoices also often leave a carbon tissue which shows the account number. These are but a few instances where the account number is accessible for later fraudulent use.

This does not mean that we in the credit reporting industry wash our hands of any responsibility if account numbers are criminally obtained from credit reports. We believe every provision of the FCRA should be enforced.

Since the early 1960's, ACB has brought the consumer credit industry together to find solutions for previously unforeseen problems. We accomplished this with the Fair Credit Reporting Act and on the issues of file integrity and file security. It is also our intent to have this issue of credit card fraud, coupled with the need to properly identify accounts and consumers, addressed by an inter-industry task force under the banner of the Credit Grantor Advisory Group of Associated Credit Bureaus.

Thank you, Madam Chairman, for the opportunity to discuss this issue with the Subcommittee. After Mr. Baker's and Mr. Price's remarks, we will be happy to answer any questions.

Senator HAWKINS. Mr. Baker.

STATEMENT OF JOHN BAKER, PRESIDENT, THE CREDIT BUREAU, INC., ACCOMPANIED BY BRIAN GARRETT

Mr. BAKER. Thank you, Senator Hawkins.

[Complete statement follows:]

STATEMENT
of
JOHN BAKER

Senator Hawkins and Members of the Subcommittee, my name is John Baker, and I am President of The Credit Bureau, Inc. of Georgia, or CBI, as we are more generally known. Accompanying me today is Brian Garrett of our Corporate staff.

We appreciate this opportunity to express our views at these hearings on credit card fraud, a growing problem which has been estimated to cost consumers and businesses hundreds of millions of dollars annually. We believe that it is vitally important that any new law aimed at preventing credit fraud should not unduly restrict the use of account numbers in the consumer reporting and collection business. As I will explain, account numbers are an integral and essential part of the consumer reporting process which is adequately governed by the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) ("FCRA") and credit industry practices.

CBI

Before commenting on consumer reporting agencies' use of account numbers, let me give you some additional information about CBI. CBI provides consumer reporting and related services to American businesses. We are a "consumer reporting agency" as that term is defined in the FCRA. Our operations are typical of today's automated consumer reporting services which assist business in the analysis and management of financial risks, and which help consumers obtain the goods and services they want and need.

CBI has 31 automated credit reporting centers in 22 states. We have 50 sales and service locations. We also have 110 independently owned bureaus which use our automated reporting system, and 31 individual collection offices. Our system serves over 50,000 credit grantors who use about 35 million consumer reports annually.

Every day approximately 1,000 consumers ask CBI for disclosure of our file information about them, a right established by the FCRA. In 1982 we disclosed files to over 360,000 individuals. The rights of consumers established by the FCRA are summarized in an appendix to this statement.

CBI is a wholly owned affiliate of Equifax Inc., a major supplier of information services to business, industry and government. These Equifax activities give the company a broad perspective on many issues of public concern. For example, information services provided by other Equifax companies and divisions aid in protecting against resume fraud, insurance fraud, employee dishonesty and fraud in the receipt of public funds. In each instance the ability of customers to obtain information acts as a deterrent to misrepresentation and is a means to detect attempted fraud. The same is true of credit fraud -- the availability of current, accurate information can help the credit grantor detect fraudulent applications for credit.

Credit Fraud and Security Procedures

According to the growing body of experience and information about credit fraud, major methods by which such frauds are perpetrated include dishonest employees, unauthorized use of stolen or lost credit cards, counterfeit or altered cards, fraudulent applications and fraudulent orders by telephone or mail. Most of those credit frauds -- such as the unauthorized use of a card or the making of counterfeit cards -- generally have no connection with the consumer reporting industry, and are not within the range of our direct experience.

Our stringent security procedures keep fraudulent activities in the consumer reporting process to the absolute minimum. In those rare instances when we encounter falsified credit records, it is our practice to report the situation to law enforcement officials so they can take appropriate action. Our security procedures include physical security measures and the use of business account codes, unique operator access methods, security code numbers and automatic billing -- which includes the exact time and identity of the person accessing the file. Our internal procedures require special pass words to obtain access to files, and only certain restricted supervisory terminals are permitted to perform certain transactions. Our customer's terminals cannot change the file names or modify the account information in our credit files. Audit trails are made of all changes to the system, and random audits are made of changes to file data made by our personnel. In short, we have very extensive and effective security procedures to prevent fraudulent situations in connection with consumer reporting agency data.

Legitimate Uses of Account Numbers

One means that has been suggested to protect against credit frauds involving account numbers is to prohibit the disclosure of credit account numbers, except in certain limited circumstances. We recognize that the Subcommittee might wish to take this approach. However, we urge that you first carefully consider the views of creditors to learn if such a broad prohibition would be too restrictive to accomodate necessary business practices. In addition, we ask that appropriate exceptions be made for uses of account numbers by consumer reporting agencies. Reporting agencies must utilize account numbers in various ways as set forth below. We believe that there are adequate protections in existing law and business practices to obviate the need for additional restrictions on our use of account numbers.

I believe it now will be helpful to describe legitimate uses of credit account identifiers such as name, address and account number, which are directly related and essential to the operation of an automated consumer reporting agency. Each of these uses is well established and is recognized as appropriate under the FCRA and state laws, which have established specific protections against the misuse of information in our business. These established legitimate uses of account identifiers, which are vital to the credit and collection process, include the following:

1. Communication to consumer reporting agencies. Most major credit grantors provide automated credit bureaus each billing cycle with magnetic tapes containing the customer account status as shown on each of their customer's monthly statements. This information is then programmed by our company to assure a standard format for processing by our computer system. The account number is used to assure that a correct matching occurs. More current information automatically replaces older information, and the history of the account is preserved. When all tapes have been run, the credit file has been updated. Special precautions are taken to review the information on each tape and compare the statistics with prior months statistics. Random accounts are verified by information from prior months or by contact with the supplier directly. This quality control process helps us to assure accurate handling. As a result of these activities, possible only in an automated environment, credit reports are accurate, current and provide a fair and comprehensive picture of a consumer's account status with his or her creditors.

The process, of course, can only work if complete acccunt identifiers are communicated to the bureau. It is a matter of concern to us that a tape containing account information could itself be considered a prohibited list of account identifiers in any possible legislation. Communication to consumer reporting agencies is as important as communication by consumer reporting agencies.

2. Communication by consumer reporting agencies. The heart of each individual credit report is the current status of each credit account that is created as I have just described. We provide reports only for legitimate business purposes as specified by the FCRA. The FCRA, in addition to many other consumer safeguards, provides stringent protections against improper disclosures of report data, including a consumer's account numbers. Thirteen years of experience has shown that the FCRA works well.

3. Communication between consumer reporting agencies. Any proposed law must preserve the ability of one consumer reporting agency to communicate with another, and this communication, too, is based upon account identifiers. The communication of information between bureaus is necessary so that consumers may have the benefit of former address information when they move and so that information is available in the event they are using credit in a location

away from home, or using an account from another location as a reference.

4. Collections. The communication of account identifiers is necessary in the collection process as well. Debt collectors are required by federal and state laws to verify the debts and to maintain segregated accounts in the case of the multiple debts, and account numbers are an important tool in this process. Collection assignments are frequently communicated in automated form similar to accounts receivable tapes.

5. Account monitoring services. Automated bureaus offer account monitoring services so that creditors may review the overall credit status of their current customers. This service can help spot a flurry of credit activity perhaps resulting from criminal use of lost or stolen or counterfeit cards or from other fraudulent activities such as "loading up" in preparation for elective bankruptcy. As the name implies, the account number is a key identifier.

6. Credit marketing services. Consumer reporting agency data is also used for marketing purposes. In our competitive business environment, credit promotions help mer-

chants and other businesses succeed. For example, the solicitation of individuals to open new credit accounts is an important activity for credit grantors and consumers. Merchants want credit business and consumers want the ability to buy on credit. Frequently, the most convenient way for consumers to open a new account is in response to an offer from a merchant rather than making an individual application. Since the ability to use credit at the store is a definite attraction, the store's marketing plan often includes an offer to extend credit to as many potential customers as possible. Through a computerized matching of the geographical area from which the store expects to draw customers with criteria indicating a satisfactory payment history elsewhere, a list of names and addresses of qualified credit prospects can be generated. The same procedure applies when the customer is a card-issuer or other type of business, other than a retailer. It is important to note that CBI does not provide account numbers with the list of qualified prospects.

7. Consumer disclosure. Another important use of account identification is in the consumer disclosure process as provided by the FCRA. The specific use of account numbers in consumer disclosure situations is particularly important. Individuals may have more than one account with a financial institution, and we must have

the account number to make the proper distinctions. The account number is also needed for contact with the creditor to reverify the accuracy of information. Although the account number is not technically needed for the disclosure of the "nature and substance" of information to a consumer as required by the FCRA, the disclosure of specific file details is usually preferable. It has been our experience that showing an individual a report overcomes the occasional suspicion that something is being hidden. Anything blanked out or changed can be suspect. Visual inspection or mail disclosure of the complete report, including account numbers, is required in some state versions of the FCRA, including those of California, Maine, Maryland, New Hampshire and New York.

CONCLUSION:

More than a decade ago, in enacting the FCRA, the Congress found that: "The banking system is dependent upon fair and accurate credit reporting," and that "(c)onsumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers." Today, consumer reporting agencies play an even more essential role in our credit-oriented economy. Therefore, while seeking ways to prevent or deter credit fraud, the legitimate uses of credit account information which I have described must be allowed to continue. The systematic use of credit reports itself provides a strong deterrant to credit application fraud by offering an independent verification that the facts presented in an application are true. Credit reports also give a picture of the total consumer debt load and capacity, which otherwise would be unknown and which may have been misrepresented on the application.

Both business uses and consumer disclosures are already specifically addressed in the FCRA, which establishes penalties for the misuse of information. An individual who obtains information from a consumer reporting agency under false pretenses is subject to a $5,000 fine or one year in prison or both. The same penalty is applicable to an employee of a consumer reporting agency who releases information improperly.

Certain statutory protections also already exist for the consumer whose credit card is misappropriated. However, the credit grantor must absorb losses above a minimal amount -- which, in the long run, impacts consumer prices. CBI believes that any new statutory remedies proposed should allow the private sector the necessary flexibility to respond to new and/or modified fraud schemes as they emerge. Credit criminals are innovative and persistent and mere statutory prohibitions will not stop attempted violations by professional criminals. In many cases, account identifiers and other information will be needed to combat these frauds. Card issuers, their security departments and associations as well as consumer reporting agencies are actively seeking ways to detect and limit fraud. Any legislation should compliment their efforts by recognizing and encouraging the exchange of information between credit grantors and reporting agencies.

We appreciate this opportunity to share our perspective on this complex problem of credit fraud. I would be happy to answer any questions you may have.

SUMMARY OF RIGHTS PROVIDED BY THE FAIR CREDIT REPORTING ACT AND CBI's FAIR INFORMATION PRACTICES

The availability of prompt, low cost, factual information to help creditors evaluate probable willingness and ability to pay is a positive factor enabling consumers to purchase a wide array of goods and services offered in our economy. Our reports help business serve consumers and consumers enjoy specific individual protections under the FCRA, State laws, and CBI's own Fair Information Practices. The FCRA's protections include:

-- A reporting agency may issue a consumer report only for a permissible purpose set out in the Act -- a business transaction involving personal, family or household needs.

-- Whenever an individual is denied a benefit, or pays more for that benefit, because of information supplied by a reporting agency, he is notified of that fact by the user, and supplied the name and address of the reporting agency.

-- A reporting agency is generally prohibited from reporting adverse information over seven years of age. The exceptions are: that bankruptcy information may be reported for 10 years, and when credit or insurance transactions exceed $50,000, or, for employment purposes, when the annual salary exceeds $20,000 such information may be reported.

-- A reporting agency must follow reasonable procedures to assure maximum possible accuracy of report information.

-- Public record information which is likely to have an adverse effect is reported for employment purposes, must be down to date at the time it is reported.

-- Reports may be submitted to a governmental agency only for one or more of the permissible purposes enumerated in the Fair Credit Reporting Act.

-- A consumer can obtain disclosure of information from the consumer reporting agency.

-- A reporting agency must reverify, when necessary, any file information that is disputed by the consumer.

-- Information which cannot be reconfirmed must be deleted and a corrected report sent to previous recipients of the information within the previous two years for employment purposes and the previous six months for any other purpose.

-- A consumer has the right to make a written statement concerning reconfirmed information, and any statement must be included in all future reports.

-- A consumer who feels that he has received incomplete disclosure or who has suffered some other abuse may file a complaint with the Federal Trade Commission, which has responsibility for the enforcement of the Fair Credit Reporting Act.

-- The consumer is entitled to monetary compensation for any reporting agency's willful abuse of the FCRA's provisions.

We are convinced that existing protections are more than adequate, and embody the key principles of fair information practice and confidentiality.

The laws of several states require methods of consumer disclosure not specified in the FCRA, including providing copies of reports in person or by mail. In other states, on a voluntary basis, CBI will use these disclosure methods when to do so seems to be the best way of resolving the consumer's problems. Additionally, we do not charge for disclosures in all instances where charges are permitted under the law. It is our aim, as it is the intent of the FCRA, to make the consumer disclosure/dispute/reinvestigation/correction process an effective procedure to promote accuracy in reporting, and our fair information practices, based upon our experiences with hundreds of thousands of consumers, are intended to enhance this goal.

It is of special interest in the context of these hearings that the FCRA establishes standards of confidentiality and penalties for violations of confidentiality. When information from the files of a consumer reporting agency is disclosed or obtained without a permissible purpose, the penalty is up to $5,000 or a year in jail. These penalties, plus our own employee awareness programs and security procedures, make compromise of consumer report information extremely rare.

Senator **Hawkins**. Thank you, Mr. Baker.

Mr. Price.

STATEMENT OF WILLIAM B. PRICE, PRESIDENT, CBC COS., INC., COLUMBUS, OHIO

Mr. **Price**. Madam Chairman, my name is William B. Price and I'm president of CBC Companies of Columbus, Ohio. The CBC Companies are a privately-owned concern comprised of 25 credit bureaus in Ohio, Pennsylvania, New Hampshire, West Virginia, Indiana, Maryland, Michigan, and Vermont. We employ approximately 550 people and issue approximately 6 million credit reports per year. We are unique in the credit reporting industry in that we utilize four of the five computerized credit reporting systems—Associated Credit Services, the Chilton Corporation, TRW Information Services, and Trans Union Credit Information Company.

Mr. Baker and Mr. Kurth have detailed the use and the workings of the credit card numbers in our industry. You have my written statement. I will at this point pause and open myself for questions.

[Complete statement follows:]

STATEMENT BY WILLIAM B. PRICE

PRESIDENT OF CBC COMPANIES, INC.

COLUMBUS, OHIO

Madam Chairman and Members of the Subcommittee on Consumer Affairs of the Senate Committee on Banking, Housing and Urban Affairs, my name is William B. Price and I am president of the CBC Companies of Columbus, Ohio. The CBC Companies are a privately-owned concern comprised of 25 credit bureaus in Ohio, Pennsylvania, New Hampshire, West Virginia, Indiana, Maryland, Michigan and Vermont. We employ approximately 550 people and issue approximately 6 million credit reports per year. We are unique in the credit reporting industry in that we utilize four of the five computerized credit reporting systems -- Associated Credit Services, the Chilton Corporation, TRW Information Services and Trans Union Credit Information Company.

As you heard in the preceding testimony by Associated Credit Bureaus, Inc. (ACB) and The Credit Bureaus, Inc. (CBI), account numbers play a significant role in the credit reporting process. That process is not one which is onerous or mysterious but one which, in fact, has been discussed by this subcommittee periodically and in some depth since the late 1960s when hearings were heard on a bill sponsored by Senator Proxmire. I was pleased to present testimony on that bill, which ultimately became the Fair Credit Reporting Act (FCRA) and went into effect in 1971. Since that time, credit reporting has received its share of the limelight through attempts to amend the FCRA, enforcement activity by the Federal Trade Commission and news stories in the press.

These activities, I feel, and the open and forthright manner with which the industry has dealt with them, illustrates an important point: credit reporting is an above-board business with a significant impact on the American economy.

That the industry has such a great impact is due largely to the fact that its stock in trade is providing accurate credit information to credit grantors. Not only is it our stock in trade, it is also a mandate of Section 607 of the FCRA, which requires consumer reporting agencies to "follow reasonable procedures to assure maximum possible accuracy." As has already been mentioned, computerized credit reporting companies have established a number of procedures for compliance with this section of the law. Of course, one of the most crucial concerns is that a consumer's account information ends up in his or her file and not someone elses. This process depends on adequate identifying information such as name, address, former address and social security number. Account numbers are an integral part of that identifying information due to the need for adequate information to link the consumer with his or her exact account. Account numbers also, as you know, play an important role in updating, correcting and, if necessary, deleting credit information from the file as provided for in the FCRA.

Equal to the desire of the industry to provide account information is the recognition that confidentiality of the information must be preserved.

The thrust of protecting that confidentiality in the early 1970s was directed at prohibiting confidential information from getting into the hands of someone lacking a legitimate purpose. Hence, Section 604 of the FCRA outlines the permissible purposes for which credit bureaus may issue reports. Furthermore, Section 607 requires credit bureaus to maintain procedures to avoid violations of Section 604.

Subsequent to the passage of the FCRA, the industry has been concerned with confidentiality of information from the standpoint of fraudulent use of that information. It is that fraudulent use that I understand is the subject of concern of this subcommittee. It seems that no sooner does the industry devise a method to guard against one type of fraud than another is perpetrated.

For example, ingenious attempts and schemes have been devised whereby consumers or organizations representing consumers attempt to alter a credit history by exploiting well-meaning provisions of the FCRA. If this effort is successful, it may lead a credit grantor to an erroneous decision of granting credit to an otherwise unworthy customer. Thus, we have taken numerous steps as an industry and as a company to protect against this.

Like my colleagues Mr. Kurth and Mr. Baker, if there is some way I can be of assistance to minimize or eliminate the misuse of account numbers I stand ready to work out a solution with you and all concerned. At this time I believe I can be more helpful in my testimony by responding to your questions and helping to identify how our industry might play a role in working toward alleviating this problem.

Thank you.

Senator **Hawkins**. Thank you so much.

We have a lot of information now in this record and I'm sure that there are a lot of differing viewpoints. Before we frame the legislation, I desired to get all the viewpoints in the record and then have a subsequent meeting to iron out the different interests that each of us has. The overriding interest, of course, should be protecting the consumer. I think it's obvious that we have seen today, but not for the first time, many dramatic examples of the alarming increases in the fraudulent use of credit cards.

It's very prevalent in my State with a high traffic of tourists and in heavily transient areas such as New York, but it is spreading throughout the country as organized crime becomes involved.

IMPROVEMENT IN THE VERIFICATION PROCESS

One witness testified that the industry could do a lot to improve the verification process. Do any of you have any comments on that?

Mr. **Baker**. Which verification process?

Senator **Hawkins**. Verification as to if this is really that person's card. I was wondering if you had any insight into that coming from the retail side.

Mr. **Baker**. Well, I'm sure this is responsive to your question because I'm not sure we would be able to see it from the point of view that that particular comment was made, but the verification process primarily that we provide is to make sure that the credit man can verify the information that's actually put in the application where the applicant says, "I owe these following bills and I have not had difficulty with them" and so forth.

Mr. **Schober**. Well, the authorization systems used by many of today's retailers are indeed quite sophisticated and one was telling me the other day, one of the major retailers, that their system of communication nationwide in their stores and their credit authorization centers was almost like MCI as far as the communications lines go, that they were fully automated and you could present a card in a store in Philadelphia even though your account may be carried in the Los Angeles credit center, and you could still get verification in 6 seconds.

Now, to be sure, there are many others who simply cannot afford that type of authorization system, particularly the small local merchants. It's a matter of cost, Senator, and the bigger retailers generally have been able to implement very sophisticated authorization systems.

But I will hasten to say, as far as we can tell, the incidence of credit card fraud for retailers is not as great as it is for three party cards. Yes, there is fraud among retailers and, yes, we do get ripped off, I think the real focus is not on the J.C. Penney card or the local F. W. Woolworth card. It's on the cards that are honored by many merchants and on which there's a cash advance privilege which retail cards do not have.

IMPACT OF PROHIBITION ON THE SALE AND DISTRIBUTION OF LISTS

Senator **Hawkins**. The Director of the Consumer Affairs Office of Palm Beach, Mrs. Skaggs, has brought to our attention the fraudulent use of lists with names, addresses and account numbers. So she recommends that we introduce legislation to prohibit absolutely the sale and distribution of such lists. Although the Federal laws prohibit the fraudulent use of credit cards, they dc not apply to account numbers.

What effect would the absolute prohibition of the distribution of such lists or any part of such lists have on your industry?

Mr. SCHOBER. Well, as we pointed out in our prepared testimony, there are many legitimate uses of lists. If you prohibit the use of lists for marketing purposes—I'm not talking about account numbers; I'm talking about names and addresses—what you're doing effectively is building in a competitive advantage for the existing merchants and you are fencing out newcomers in the field because the way you build a business whether you're selling merchandise or whether you're trying to develop an account base for your own in-house credit accounts or whatever you're trying to do to get ahead in merchandising, advertising is the name of the game, and if you prevent lists from being used, then you're locking in the existing advantage of existing merchants.

After all, merchants don't use lists just because they like to pay postage. They are very sophisticated in choosing the lists they use, the list that is most likely to generate the most business. Retailers want a person to open that mailing piece and to be pleased by what he or she sees and to come in and buy or to come in and open an account, but in some way respond affirmatively.

So the lists are not used helter-skelter, willy-nilly. They are very carefully targeted to produce maximum results.

Senator HAWKINS. Thank you, gentlemen, so much for coming today. I think what we have learned is that we need to clarify the Truth-in-Lending Act and your information and testimony today will help me in drafting my amendments to the Consumer Credit Protection Act. We thank you so much.

[Whereupon, at 12:30 p.m., the hearing was adjourned.]

[Additional material supplied for the record follows:]

TESTIMONY OF ALICE C. SKAGGS, DIRECTOR, CONSUMER AFFAIRS OFFICE OF PALM BEACH COUNTY, FLA.

Madam Chairman and Senators, I regret that I cannot appear before you personally to respectfully request that you consider the urgency of my statements.

On August 5, 1982, Palm Beach County's Office of Consumer Affairs was notified by the Economic Crime Division of the State Attorney's Office, 15th Judicial Circuit of Florida, that they had received three complaints against a firm who bore several names. Those names were "One Step Protection" by "Credit Mutual", "Credit Marketing, Inc.", "BankCard", headquartered in Sarasota, Florida.

The allegations were that the consumer complainants had found a $49 charge on their credit card statement made by these companies for alleged credit card protection, that the complainants had allegedly neither ordered nor authorized. The complainants stated that they had received phone calls from these firms offering the credit card protection service, but the complainants denied having ordered the service or having authorized the charge against their credit cards.

In an effort to ascertain how widespread these alleged charges might be, I did impromptu surveys of several groups of people who attended my speaking engagements within the next several weeks. I also made an appeal on TV and on radio, that I might be made aware of anyone who had a similar complaint. During this impromptu, and certainly unscientific, survey, I learned that while 75 percent of those present owned and used credit cards, 25 percent never checked their monthly statements. Consequently, it is logical to assume the likelihood of 25 percent of those billed, simply paid for the service without their knowledge.

The final result was that this office received 153 written and sworn statements of complaints.[1]

Shortly after August 5, 1982, I had contacted Assistant State Attorney, Barbara Briggs in Sarasota, to inquire about this company. Attorney Briggs advised me that their office was also receiving complaints. Thereafter, I received a phone call from a bank attorney in Tampa by the name of Barbara Louks, who informed me that Tampa was also receiving complaints. Sometime later, an individual from a Tampa bank phoned me and alleged that a number of banks in Sarasota and Tampa, were being defrauded by this firm in an engenious manner. It was alleged that the firm would make very large deposits in a bank, via their credit card telephone order slips, which, of course, are treated as cash, and would then withdraw these deposits prior to the 60 day turnaround on the credit card charge, leaving the bank to suffer the losses.

It was alleged that more than 25 banks in Sarasota and Tampa had been defrauded in this manner. These are hearsay allegations. However, the Tampa office of the FBI, in the person of William Smith, Sarasota agent, were, indeed, involved in this investigation.

All credit card companies involved nationally, removed the unauthorized charges from the credit card holders statement.[1]

About the first week of December, 1982, upon completion of our investigation, the entire matter was handed to Assistant Attorney General, Leonard Elias of the Flordia Department of Legal Affairs, the chief law enforcement officer of the State of Florida. On December 28, 1982, Attorney General, Jim Smith, issued a Cease and Desist Order on the above referenced firm.[4]

That Senators, is a thumbnail sketch of how the Office of Consumer Affairs, and I, as it Director, became involved. My investigation showed, and Credit Marketing stated during newspaper interviews, that they had purchased lists of credit card holders names, addresses, credit card numbers, and information. Obviously this was taken from the original applications of the complainants. By their own admission, they allegedly made 300,000 to 400,000 sales calls a month, claiming that the unauthorized charges were simply human error. If that be the case, they were able to acquire thousands upon thousands of credit card holders names and credit card numbers.

Senators, the mere fact that this company or any other person or company has the ability to acquire your credit card number and mine, is an indignation, and it is a disgrace for us to be placed in the position of expecting anyone to make that information available to a third party by simple selling the lists.

I am appalled and infuriated because I feel very strongly that my credit card, and yours, and all others, should be protected by the Privacy Act. Without that protection, it seems akin to permitting anyone the unauthorized use of my money, for certainly, a credit card is a valuable document and is, indeed a substitute for cash.

While I recognize the limited need by financial institutions, to furnish credit information to credit reporting agencies, credit collection agencies, and the like, I also recognize the posssibility that this information is put into a computer, and the strong probability that someone else may buy a terminal in that computer and delete from the computer, and information they choose to acquire.

As for merchants of all sorts, including mail order, having the right to sell credit card lists, is, in my opinion, an abomination, and certainly an invasion of my privacy.

Yet another problem is inherent in the present from of credit charges sales ships. The sales slips are in triplicate and include two carbons. One of the easiest ways of fraudently using a credit card, is for the "con artist" to check dumpsters behind the businesses and retrieve the carbon copies of all credit charges for that day, and use those credit card names and numbers to order merchandise to be mailed to themselves.

In West Palm Beach, we recently had such an occurrence whereby a young man from North Carolina spent the entire winter in a hotel in West Palm Beach by operating in just that manner, and selling the merchandise that he had ordered on peoples credit cards.[2]

In an effort to hopefully eliminate this problem, I strongly recommend that all credit card charge slips be made of (no carbon required) NCR paper, thereby eliminating the need for the inserted carbons.

---

[1] See Exhibit A.

[2] See Exhibit B.

[4] See Exhibit D.

As a point of information, when President Reagan visited Miami, Florida on November 16, 1982, members of ABC, NBC and the Wall Street Journal, after leaving Miami, learned that their credit cards had been fraudulently used, yet they still possesed their credit cards. The possibilities of how it happened, are numerous, but the simplest method would be the use of the carbons used for their credit card charges.

While I am well aware of the opposition that will be generated by the proposal being made to this Subcommittee concerning credit card fraud, I am cognizant of the fact that many companies need to purchase mailing lists, to which I have no objection. However, I can see no logical reason for those mailing lists to include credit card numbers. Consider for the moment, the fact that financial institutions are not permitted by the Federal Privacy Act to give anyone your bank account number, yet there is no law against providing your credit card number.

Senators, there is an eight billion dollar annual loss to the consumers through credit card frauds in this nation.

Some gasoline companies are charging 3 percent in addition to the cost of the gasoline, if a credit card is used, or they will give a discount for cash. I was appalled at receiving an offer from one of these companies to extend me a credit card, and I questioned that company as to the reason for their charging 3 percent for the use of credit cards. The response was that their losses on their credit card business were so great, as to make this 3 percent charge necessary. Yet, quite illogically, they were soliciting credit card business. This was certainly illogical in my opinion, since you don't solicit the use of an item which is repeatedly losing money for your company.[3]

You will find in Exhibit D, a newspaper article from the Ft. Lauderdale Sun-Sentinel, describing the arrest of 30 individuals involved in a credit card scam that apparently appeared ingenious to the "Con Artists". Additionally, in this exhibit, there are copies of several newspaper articles concerning this entire credit card fraud matter.

Senators, in closing, may I thank you for your attention to and concern of this matter, and I extend my appreciation to Chairman Paula Hawkins for the opportunity to testify before the Subcommittee.—ACS.

EXHIBIT A

INTER-OFFICE COMMUNICATION,
OFFICE OF STATE ATTORNEY,
August 5, 1982.

To: Alice Skaggs, Department of Consumer Affairs.
From: Harvey S. Jacobs, Economic Crime Division.
Re Credit Marketing Inc. d/b/a One-Step Protection.

In response to the enclosed complaints, I contacted Mr. Sickle, Vice President, Customer Service for Southeast Banks (833-3828). He was aware of the problem and has personally been trying to shut these people down. Apparently, he has been partially successful in keeping them from using Florida banks for their scheme as they now may be processing through Columbus Bank and Trust in Georgia.

Mr. Sickle has also spoken to a Mr. Robert Shinkle in Operations Support, VISA USA, INC., P.O. Box 8999, San Francisco, California 94128, (415) 570-3558. To date I have not been able to contact Mr. Shinkle.

Mr. Sickle advised that when a consumer complains they are credited for the amount charged and the processing bank is then responsible for debiting the merchant's account (in this case, One-Step), however, One-Step closes its compensating account at the bank before all of the reversals can be debited. Therefore, the bank gets stuck. However, if consumer doesn't complain or doesn't reach correct person bogus charges remain.

Investigation continuing.

HARVEY JACOBS.

ACTION REPORT

Subject, One-Step Protection; Date, July 30, 1982; mode of contact, phone; Reporter, Shirley; time, 11:00 p.m.

Source: Kirby Mole, 112 Santiago Street, Royal Palm Beach, FL 33411; Phone 793-6393 (work), 793-5761 (home).

---

[3] See Exhibit C.

One-Step Protection, by Credit Mutual, called him on the phone and wanted to sell him insurance on his Master Card in case it was stolen. (The bank where you got your card states in its terms that you will be be liable in such case for no more than $50.00; this company, for a fee of $49.00 will cover you so that you don't have to pay that initial $50.00!!) He told them that he did not want their protection. He also notified Southeast Bank who issued the Master Card that they were not to honor any charge by this agency as he had told them he did not want the coverage. He received a letter from One-Step telling him that he would be receiving a "kit" in the mail concerning his coverage. He sent a letter to One-Step telling them not to send the "kit", that he did not want the coverage. Today he got his Master Card statement and on it was a charge for the $49.00 (it is listed on the statement as Credit Marketing Corp., Grand Prairie, Texas, but the bank verified that that is the same as One-Step Protection). He called Master Card and they are going to remove the charge from his statement (then he cancelled the card). The bank told him that they have had other complaints on One-Step. The person he talked with at Southeast Bank is Mrs. Palant, Southeast Services, Inc., Customer Service, P.O. Box 523500, Miami, FL 33152, #1-800-432-1038. The person he talked with at One-Step was Mike Richards, 1718 Main Street, Sarasota, FL 33577.

Mr. Sickle, from investigations will call.

ACTION REPORT

Subject, One-Step Protection; date, August 4, 1982; mode of contact, phone; reporter, Shirley; time, 11:00 a.m.

Source, Marian McClenaghan, 9160 Banquet Way, Lake Worth, Fl. 33463; phone 439-4392.

Ms. McClenaghan was contacted by phone by One-Step, wanting to send her a "kit" concerning insurance on her Visa card. She tried to get some information from them, and started getting transferred from person to person, sometimes getting hung up on and sometimes being told she would have to call back. She supposedly talked with a supervisor, and when she tried to find out how they got her name and credit card number, she was told it was from a list they had bought, and when she tried to find out from whom the list was bought she was told he did not know and even if he did know he would not tell her, and then got extremely rude to her.

The number she was told to call at one point was 1-800-282-2270.

ACTION REPORT

Subject, One-Step Protection; date, July 28, 1982; mode of contact, phone; reporter, Shirley; time, 4:00 p.m.

Source, Donna Lane, 1030 U.S. No. 1, Apt. 109, North Palm Beach, Fl. 33408, phone 627-1718.

One-Step Protection called her and wanted to sell her insurance on her Visa card, offering 100 percent coverage in case her cards were stolen or lost. She said she did not want the insurance, but when she got her monthly statement, they had two charges on there for $49 + for the coverage. She reported it toVisa (Visa, P.O. Box 30035, Tampa, FL., 33630) and they said that they had had a lot of similar complaints, and that maybe she should report it locally to us. They are going to delete the charge from her card.

She just thought that we should be aware of this going on, in case something could be done about it. She does not have an address or phone number for One-Step. She only knows, because of the charge on her statement, that it is located in Sarasota, Fl.

DELRAY BEACH, FLA.,
October 25, 1982.

PALM BEACH COUNTY STATE ATTORNEY,
Investigations Division, South County Courthouse
Delray Beach, Fla.

Regarding unauthorized charges to credit card accounts for a credit card protection service. On our Sept. 1982 Master Card statement, we were charged $49.00 by Credit Marketing, Inc. of Galveston, Texas. Calling the 800 number for Master Card, I informed them we did not make this charge and, at their request, I immediately sent a letter to Master Card, Card Holder, Merchant Claim Dept. stating this was an unauthorized charge. We received an answer from them that this matter would be looked into, etc. The $49.00 charge plus a $2.32 finance charge were on this months (Oct) statement.

We felt that your office would be interested in knowing that charges are also coming from Credit Marketing, Inc. of Galveston, Texas. We are respectful of our credit cards, know our purchases and check our statements, but this causes concern and the convenience of credit cards are nil.

We would appreciate any advice or help you can give us regarding this matter.

Sincerely,

ROBERT J. MCCOMB.

THE AMERICAN CIVIL DEFENSE ASSOCIATION,
Starke, Fla., September 28, 1982.

OFFICE OF THE ATTORNEY GENERAL,
Tallahassee, Fla.

GENTLEMEN: I enclose a letter I have addressed to "Credit Mutual Int." in Sarasota. I felt the office of the Attorney General should be aware of this.

Sincerely,

MAX KLINGHOFFER, M.D.

MARATHON, FLA.,
September 28, 1982.

CREDIT MUTUAL INT.
Sarasota, Fla.

I have received a postcard stating that you are billing me, through my Master Card, for "one step protection".

Please be informed that I have not authorized such a transaction, and I do not wish to purchase this "insurance". I have already contacted the office of Master Card, and have been instructed not to pay for this.

In my opinion there is fraud involved in charging for a purchase which was not authorized.

Sincerely,

MAX KLINGHOFFER, M.D.

ONE STEP PROTECTION,
Sarasota, Fla.

Congratulations on your decision to join thousands of other credit card holders in the fight to protect against theft, loss and fraudulent use of credit cards.

This notice serves as confirmation that your protection has been in force since 9/25/82 when during a phone conversation with our representative you acknowledged your desire to enroll in One-Step Protection, a credit card registration and protection service.

Your enrollment kit will be mailed to you shortly.

Your membership is for seven years and covers all credit cards that have been issued or will be issued in the future to you and your immediate family.

You will be billed $49.00 for your membership on your VISA/Master Card account.

If you should lose your credit cards or have any questions please contact our Mr. Richards: Credit Mutual Int., 1718 Main Street, Sarasota, FL 33577.

Telephone Sales Representative #3319.

EXHIBIT B

September 1, 1982.

MRS. SKAGGS: Enclosed letters are Self-Explanatory! After my husband received letter of August 12th 1982 from Ginger Moran—I began working on it. I traced the accurate address to the Dixie Court Hotel. I checked out the phone number—305-832-9235 and the Telephone Operator told me—it was a coin operating telephone. I don't think she believed me when I said it was a fraudulent matter and therefore would not give me any more information. I called Ginger Moran of the Blue Angels and gave her what information I had. I suggested she call the West Palm Beach Department and gave her their telephone number. I told her they would have the authority to go inside the Dixie Court Hotel and ask some questions whereas I did not have the authority. She followed thru with my suggestion. She sent us the next letter on August 19th 1982 with the information she received.

Today I sent copies of the two letters from Ginger Moran to one of my husband's patients who works for the Telephone Co. I have asked her if she would contact Ginger Moran and perhaps let here know where the telephone number is located inasmuch as it was a fraudulent matter.

I am just wondering if that phone number might not be inside the Dixie Court Hotel! In the meantime—on my day off each week—I am showing Ginger Moran letter of August 19th to Store Managers of Departments Stores—so that they realize by their carelessness of throwing away carbon copies of sales (charges) and voids—into their dumpsters without destroying them first—what is happening to we people the consumers. How it enables another Scam Operation to become very effective.

I am bringing this matter to your attention so you are aware what is going on not only in our community but elsewhere.

I am continuing to follow thru with this matter—not only in protection of—my husband and myself—but for all other innocent peoples who are caught in this Scam procedure. So far it was taken 7 months of my time because of a Department Stores carelessness. Thanks. We are blessed in our Community to have people like you—dedicate themselves to matters such as this Scam operation.

CAROLINE SAUER.

BLUE ANGEL, INC.
Charlottesville, Va., August 12, 1982.

EDWARD SAUER,
West Palm Beach, Fla.,

DEAR EDWARD SAUER: I'm writing about the use that was made of your name and MasterCard credit card number to charge an order from our company. In January, 1982 we received a phone order for a large record set, the Original Hendrix collection at a cost of $69.99 plus $3.00 shipping. We called the bank and they approved the use of the number, so we went ahead with the shipment. It has just come to our attention that your bank has been notified that this order was placed by an unauthorized purchaser.

I'm very sorry for any inconvenience this might have caused you. It seems this is the price we pay for the convenience of bank credit cards. Although we at Blue Angel make every attempt to see to it that no fraudulent use goes by us, we can do little more than clear it with the bank before sending an order and charging it to the card.

I wonder if you could be of assistance in helping us find out who have been using your card. I'm sure you are anxious to know, too. Clearly, they have your name and number and are using them freely.

The address we were given and to which we shipped the records is 301 N. Dixie Court, W. Palm Beach. The phone number we were given (and have tried calling and gotten no answer) is (305) 832-9235. Do you have any information on who might be using this address and phone number? If you could help us out, we would appreciate it.

We will put a shipping tracer on the package and see if we can get any information on who received the package.

Thanks for bearing with us. And, again, sorry for the inconvenience.

Yours,

GINGER MORAN.

P.S. Please address your answer to the Credit Card Blues Department where this file will reside until we clear it up. Thanks.

BLUE ANGEL, INC.,
Charlottesville, Va., August 19, 1982.

MRS. EDWARD SAUER,
West Palm Beach, Fla.,

DEAR MRS. SAUER: I got your note this morning, at the same time as the returned shipping tracer from UPS. I'm sending a copy of the tracer on to you for your information.

But what is more to the point is that I spoke with a detective at the West Palm Beach police department, a Detective Sicliano, at some length last Friday and he told me that he has been pursuing the man who used your name for some time. Apparently, the man was running a large scam operation from the Dixie Hotel. He got the carbons from credit card impressions which he took from the garbage cans behind department stores in West Palm Beach and used the name and numbers for ordering items by mail which he sold on the street or to pawn shops.

The name on the tracer slip is that of the hotel clerk who, apparently, signed the UPS at the man's request.

The man, Jerry Bodell, got away before Det. Sicliano could catch him and is gone, though there are warrants for his arrest in North Carolina and Florida.

Bodell apparently did not use the same name and number very often, so your card should be okay, but you might want to have your bank issue you a new one just in case.

Thanks for your help.

Yours,

GINGER.

September 21, 1982.

DEAR MRS. SKAGGS: To bring you up to date on enclosed letter. I asked a patient of my husband who works for telephone company to have Security of Southern Bell contact Ginger Moran of Blue Angels—letting her know exactly where phone number 832-9235 is located.

Patient called me back about two weeks ago. Security did check it out. They talked to Ginger Moran of Blue Angels—Det. Sicliano, Dixie Court Hotel.

They found out following information.

Name is Jerry O'Dell—not Bodell, is 22 years old, in a wheel-chair, is a paraplegic, had 35 names in his possession (ours was one), told hotel clerk at Dixie Court Hotel these were all his relatives and had packages delivered there with persons names on pkg. from carbons from credit card impressions which he took from garbage cans behind department stores. O'Dell went back to Dixie Court and picked up list of names—not there now.

Sad! To begin his 22nd year in life in this manner.

CAROLINE SAUER.

November 1, 1982.

Dr./Mrs. EDWARD A. SAUER,
W. Palm Beach, Fla.

Dear Mrs. SAUER: Further to my phone call of Friday, October 29, with reference to the articles in the Sun Sentinel of October 28, and the Post of October 29, 1982, enclosed you will find a copy of both articles for your information.

Again, let me congratulate you for your tenaciousness and hard work in helping to resolve this matter.

A suggestion if I may; whenever you use your credit card, no matter where, insist upon having the carbon copy returned to you so that you may destroy it, for to depend upon the merchants, restaurants, or gas stations to do it of their own volition, is a mistake.

Many thanks for bringing this matter to my attention. It so happens that one of the girls that works for Haselmire Advertising in this building, was one of the people whose account was charged $200 by Jerry O'Dell for a commemorative coin that he later pawned at a pawn shop where the police found it.

Good luck and God bless.

Sincerely,

ALICE C. SKAGGS,
Director, Consumer Affairs Office.

EXHIBIT C

SEPTEMBER 10, 1981.

Re: Proposed 3 percent service charge (handling?) to become effective November 1.

Mr. ELLIS W. GUNNPLS,
Vice President, Texaco, Co.
Houston, Tex.

DEAR MR. GUNNPLS: What sort of audacious geniuses meeting in a smoke filled room, came up with the masterful stroke of charging Texaco credit card holders 3 percent service or handling charge, or whatever they want to call it, for the use of your credit card.

At this point, permit me to wear two hats. First, I am writing as the Director of the Office of Consumer Affairs for Palm Beach County, Florida. My other hat is that of a Texaco credit card customer for many years past and present, although, this present customer may indeed become a past customer, if and when this "service charge" is added to my bill.

Further, I call to your attention, the fact that you, obviously, you being Texaco Company, intend to charge your customers this 3 percent which no doubt will be charges added on top of the federal and state taxes not only for gasoline, but the federal tax on tires and the 3 percent on parts and accessories, and that can go on right down to repair services.

It seems of little or no concern to you that this will also increase the cost of gasoline to the consumers a minimum of 5¢ a gallon, which will indeed effectively put your dealers out of business with their charge people.

Is it the so-called thinking of this so-called group of geniuses who devised this plan, that the dealers should have to finance their own credit? Or, is this a ploy for Texaco to put their dealers out of business so that Texaco can then become dealers?

Has it occurred to these geniuses that this idea can, and perhaps will, mushroom through the entire oil industry?

If this gem of an idea is really imposed on the consuming public on November 1, let me be the first to tell you that speaking as one of your consumers, I shall no longer have any need for my Texaco credit card, in spite of the fact that I never use my card in a manner by which I will have to pay your 18 percent carrying charge.

This is not only an audacious proposal from an oil company whose profits have been soaring, but implies distinct possibilities that impugn the morality and integrity of the oil industry.

I am deviating from the policy of this office by drawing conclusions without first hearing the other side of the issue. I invite you and urge you to submit to me Texaco's "side of this charge".

I look forward to hearing from you at your earliest convenience.

Very truly yours,

ALICE C. SKAGGS,
Director, Department of Consumer Affairs.

TEXACO INC.
Bellaire, Tex., September 18, 1981.

Ms. ALICE C. SKAGGS,
Department of Consumer Affairs,
Commerce Building, West Palm Beach, Fl.

DEAR MS. SKAGGS: Your recent letter addressed to Mr. Ellis W. Gunnels has been referred to me for reply.

Our Credit Card operation has become very expensive over the past several years with inflation and the high cost of money, making it necesssary for Texaco to implement the processing charge in order to continue providing this service. The Credit Card enables our retailers to sell Texaco motor fuel and a variety of products and services without the burden of financing receivables or facing the inevitable credit losses.

The processing charge is not a surcharge and will not be assessed to Credit Card customers. It will be charged to retailers and wholesalers. In effect, it will spread a portion of the cost of the Credit Card system to those who benefit from it.

We recognize that the processing charge will increase operating costs for Texaco retailers and wholesalers, but business conditions have made it necessary to take this step. They are independent businessmen and women, who determine the price they charge for products and services and they may adjust their margins accordingly, but they may not add the processing charge as a surcharge item on a credit card invoice. It should be noted that the charge will be similar in type to the so-called "merchants' fee" now assessed by other credit card systems, such as Visa, MasterCard, and American Express. Also, the revenue generated by the new processing charge will not cover the entire cost of operating Texaco's Credit Card system.

Texaco is committed to provide an efficient Credit Card system. This processing charge will continue to insure this convenience.

Yours very truly,

JOANNE KING.

EXHIBIT D

[From the Sun-Sentinel, Dec. 29, 1982]

FIRM TOLD TO CEASE CHARGES TO CARDS

(By Patricia Sullivan)

The Sarasota credit card protection firm accused by more than 3,000 South Florida consumers of making unauthorized charges on Visa and Mastercards was ordered Tuesday to stop the practice or face a hefty fine.

Florida Attorney Gen. Jim Smith issued the emergency cease-and-desist order against Credit Marketing Inc., also known as Credit Mutual International Inc.

He also filed an administrative complaint against the firm, saying that it had charged consumers $49 for a seven-year credit card protection service—even after the consumers had turned down the firm's telephone sales pitch.

"The (order) will assure consumers that they will not be subjected to unfair and deceptive trade practices," said Leonard Elias, assistant attorney general in Miami. If the firm violates the conditions of the order, it can be fined up to $5,000 for each violation, Elias said.

But a CMI spokesman in Sarasota said the charges are without basis.

"In no way are these charges valid," said Mark Leiberman, director of operations. "I don't feel we've been misleading in any way."

The FBI, two state attorneys' offices, Florida consumer officials and MasterCard and Visa security forces are investigating Credit Marketing on the heels of thousands of complaints about the firm.

The complaints about CMI have also reached Washington, D.C., where the U.S. House of Representatives Subcommittee on Consumer Affairs and Coinage is considering holding a hearing on the nationwide problem of credit card fraud in Sarasota during February, a subcommittee staff member said.

CMI's "One-Step Production" offers to contact the banks and stores that issue credit cards in case the consumer's cards are lost or stolen. The $49 service lasts for seven years.

The service is sold by telephone salespeople who work in Fort Lauderdale, Tamarac, Sarasota, St. Petersburg, Washington, D.C., Denver, Los Angeles, Grand Prairie, Tex. and Westport, Conn.

People who have complained to authorities say that CMI's telephone sales force presents the "One-Step Protection" as an insurance policy, which it is not; misrepresents itself as an agency of a bank, Visa or MasterCard; tells people that the $49 fee is a "special offer" when it is actually the standard price, then bills consumers who refuse the service.

The firm has the MasterCard and Visa account numbers of the people who are called, but company official Leiberman said that it never uses that number unless the consumer gives it to the company, contradicting the testimony of consumers quoted in the attorney general's complaint.

Leiberman also said that supervisors reconfirm each order in a separate telephone call, and as its own protection against fraud, asks for the maiden name of the consumer's mother.

Barbara Flanagan, the former assistant branch manager of the Fort Lauderdale office, said that verification sometimes was simply the supervisor listening in on the end of the sales pitch when a customers said the company could send information to him or her.

"Most people are being signed up without really realizing what they're buying," said Mrs. Flanagan, who herself worked for one week as a salesperson until she was fired in March. "Most of the customers get the impression that they're only signing up for information. Salesmen told me several times that people didn't understand. It was specifically told us that you didn't explain anything unless the customer asked."

If people say that information can be sent to them, the firm automatically bills them $49. The Attorney General's Office noted in its complaint that receiving information does not obligate consumers to pay for the service.

Leiberman said the bulk of the firm's business comes from South Florida. He said the seven-year-old firm contacts 400,000 people each month.

More than 100 complaints about the firm have been registered with the Palm Beach County Consumer Affairs Office, and another 100 to 200 complaints have filtered in to other country consumer offices around the state.

Sun Banks said more than 1,000 of its credit card customers have asked them to remove unauthorized charges made by CMI on Visa and MasterCard bills since last summer. Southeast Banks said they have had 3,000 such requests.

The attorney general's actions Tuesday are civil administrative complaints, but Assistant Attorney Gen. Elias noted that it will not prevent any future civil or criminal action by other agencies.

JAMES A. GARDNER,
STATE ATTORNEY, TWELFTH JUDICIAL CIRCUIT,
Sarasota, Fla., February 15, 1983.

MS. ALICE C. SKAGGS,
Director, Consumer Affairs Office,
Commerce Center Building, West Palm Beach, Fla.

DEAR ALICE: I am enclosing a copy of a newpaper article that appeared in the Sarasota Herald-Tribune on February 11, 1983. It concerns Credit Marketing, Inc.

I am also sending a copy to Leonard Elias.

Sincerely yours,

BARBARA B. BRIGGS,
Assistant State Attorney,
Consumer Fraud Division.

[From the Sarasota Herald-Tribune, Feb. 11, 1983]

CREDIT FIRM OK'S CEASE, DESIST ORDER

(By Jack Gurney)

A Sarasota-based credit card protection firm has agreed to terms of a cease-and-desist order issued by Florida Attorney General Jim Smith. Smith is expected to sign the order before the end of the month, meaning there will not be litigation in the case.

The home offices of Credit Marketing Inc., also doing business as Bankcard Services One Step Protection, are located at 1718 Main St. The firm guarantees customers it will notify credit card issuers of either loss or theft and terminate liability.

Telemarketing (telephone solicitation) is the primary method employed by the company in sales it services. Principal stockholders John Guenther and Albert Loring of Sarasota estimate 300,000 potential clients are called each month.

"Numbers have been our problem on this matter. We do a very high volume of business, so a small percentage of complaints over misunderstandings look bad," said Loring.

"We currently have 250,000 members, 100,000 in Florida, in the plan. Over a million people have been called in Florida. We process an average of 20 cases of lost or stolen cards a day. Naturally there are going to be some misunderstandings."

Fran Barno of the Sarasota Better Business Council said there are 130 complaints on active file against Credit Marketing Inc. The council bases its count on a one-year period. In addition, there are eight recent complaints pending.

"The company has been notified on the pending cases, but we haven't heard from them yet," she said. "We will soon. They always respond. There have been no complaints about the plan itself. They apparently take care of customers. That's not the problem."

Ms. Barno said the pattern and number of complaints has remained constant. "They always involve unauthorized charges," she said. "We have cases of people who claim they were either out of town or out of the country when the charge was made to their credit card account.

"All the complaints come to us naming either Bankcard Services One Step Protection or Credit Marketing Inc. They all know who it is."

Guenther produced copies of registration forms signed by customers who later denied having purchased the plan. He said it is not unusual for an individual to buy the plan, then deny having done it and request a major credit card company or bank to stop payment.

When asked about cases of signed agreements among the complaints received by the council, Ms. Barno said, "No. It's zero on that end. We don't have any of those on file. These are people who have not signed anything and not returned the literature. They have been charged for the service and don't want it."

Sarasota attorney E. V. Dannheisser has represented Credit Marketing Inc. in negotiations with Assistant Attorney General Leonard L. Elias to draft a consent order.

"What they (Credit Management Inc.) will sign is a consent not to engage in certain practices itemized in the emergency cease-and-desist order," said Elias. "This is in lieu of litigation and a hearing. In it they do not admit to violations, but they do admit to the facts of the complaint.

"They (Credit Management Inc.) wanted to inject their policies in the consent order, but I did not feel it was appropriate. How they go about remedying various situations is their business. We're only concerned they cooperate with the spirit of the law."

"In the consent order, Credit Marketing Inc. denies having done certain acts," said Dannheisser. "The order stipulates Credit Marketing Inc. is not to engage in those acts, and in the order we (Credit Marketing Inc.) agree not to engage in the acts. Basically, we're saying we never did what the order is asking us not to do, and we're agreeing not to do them in the future."

Attorney General Smith issued an emergency cease and desist order in December.

Mark J. Lieberman, director of operations for the company, said a tighter verification procedure for sales has been in effect for almost a year.

"If a customer agrees to purchase the plan, our sales person tells them they will receive a return call from a supervisor," he said. "The supervisor verifies the customer's address, gives them a toll-free number to call if they have a problem, explains the cost procedures, and asks for a Visa or MasterCharge account number."

How the account number is obtained has been high on the list of complaints. Guenther said Credit Management Inc. buys lists of credit card numbers from brokers. The source for these brokers is sales records from direct-mail order purchases. He insists buying and selling such lists is lawful.

"Our sales representatives are paid in excess of minimum wage ($3.35 per hour)," said Loring. "There is a small bonus involved for selling the plan."

Lieberman said, "The bonus is not an invitation to cheat since all sales have to be verified by a supervisor. The supervisors are paid hourly, so they have no reason to cheat. We use service observing equipment that allows a supervisor to silently monitor a sales representative's call.

"In any business of this type a 20 percent cancellation rate is expected. But 100 percent of our sales by telephone are verified. Still, there are going to be misunderstandings. We regret them."

STATEMENT OF NATIONAL RETAIL MERCHANTS ASSOCIATION

The National Retail Merchants Association is pleased to have this opportunity to present its views on the question of what legislative action should be taken in the area of credit card fraud.

The National Retail Merchants Association (NRMA) is a not-for-profit organization devoted to research and education in general merchandise retailing. NRMA represents approximately 45,000 stores in the United States, distributing about $150 billion annually in goods and services to the American consumer. NRMA's members range from the largest chain and department stores and mass merchandisers to small specialty shops and independents. Virtually all of NRMA's members operate their own proprietary credit card systems and/or accept third party credit cards that are issued by financial institutions and companies that issue travel and entertainment cards. In view of the fact that over 50 percent of our members' sales are made by means of credit cards, we are vitally concerned with the issue of credit card fraud and related practices such as the use of account numbers to obtain goods and services without the customer's authorization.

Over a decade ago, Congress decided to allocate the risk of loss from fraudulent transactions by means of a credit card to the credit card issuer. Thus, pursuant to section 133 of the Truth-in-Lending Act, as a general rule the cardholder has no liability for unauthorized use of a credit card or, under limited circumstances, the liability can amount to no more than $50 per card. We do not advocate changing this allocation of risk because, on balance, we recognize that to do otherwise could subject consumers to potentially crippling financial losses. Even negligent consumers are protected from substantial economic loss, although all consumers ultimately pay for credit card fraud as a component of the cost of credit and the cost of goods and services. This system also makes practical sense because it carries a built-in incentive for credit card issuers to strive to reduce fraud losses. While that effort is being made on several fronts, the recent increases in the amount of credit-related fraud is alarming.

During the recent hearing on this issue it was well documented that beginning around 1980 the bank card industry began to experience a tremendous increase in the incidence and amount of credit-related fraud, as well as a significant shift in the nature of this fraudulent activity. Data was submitted by VISA U.S.A. Inc., MasterCard International Incorporated and the American Bankers Association documenting that in the bank credit card industry alone losses due to fraudulent use of credit cards rose from approximately $11 million in 1972 to over $125 million in 1982—over a 1,000 percent increase. While the limited data available to us indicates that the amount of credit card fraud involving retailers' proprietary systems is not substantial in relation to total credit sales (under one-tenth of one percent), retailers are concerned about the increase in bank credit card fraud. This is because while, as noted, some of the cost is ultimately passed on to the consumer, the merchant is subjected to an increase in costs initially by paying more in discount fees to issuers of third party cards. In addition, depending upon the contract between the merchant and the bank card issuer, the merchant does bear certain fraud losses directly. For example, merchants accepting mail orders charged to third party credit cards are often charged back for fraudulent orders. Thus, we heartily endorse this Subcommittee's efforts to find solutions to the mounting problem of credit-related fraud.

NRMA believes that a number of steps should be taken to address the problem of credit-related fraud, some of which are being undertaken by the industry at the present time. For example, associations representing bank card issuers are taking steps to control fraud by changing the physical properties of the credit card itself. The credit card is being redesigned to contain a number of anti-counterfeiting features such as fine line printing, ultraviolet ink printing, and a unique hologram covering part of the embossed account number. Among other things, these steps will make alteration of the embossed account number digits harder to accomplish and easier to detect. The bank card industry is working to reprogram authorization systems to enable those participating in the systems to better identify cardholders at the point of sale. Also, bank card issuers have added a provision to their operating rules which prohibit a merchant from providing, selling or exchanging account number information, in any medium, to any other party unless connected with the merchant's legitimate bank card business. These and other steps are being taken by the industry in an effort to reduce current credit card fraud activities.

NRMA's members are continuing their efforts to develop ways to improve their own point-of-sale authorization systems and the properties of the credit cards issued in their proprietary systems in an effort to combat credit card fraud. NRMA's members are aware of their responsibility to safeguard the account numbers of their customers and they currently take steps to restrict access to account information in a number of ways. Merchants are to a greater extent using sales slips which do not involve the use of carbons and they are taking precautions in disposing of duplicate sales slips. It is essential, however, that merchants not be required to use any one particular method of effectuating sales because of the increased operating costs that would thereby be imposed. The difficulty of operating a small business profitably today is well-known and need not be documented here. NRMA is unalterably opposed to any legislation that would have the direct or indirect effect of standardizing the way in which credit is extended, or the way in which credit transactions are written at the point of sale, because of the additional costs that would thereby be imposed upon the merchant.

NRMA does support legislation which is aimed specifically at the criminal element that is responsible for perpetrating credit-related fraud. Specifically, NRMA endorses the financial community's proposal to amend the Truth-in-Lending Act and the Electronic Fund Transfer Act to fill certain gaps in that legislation. The Truth-in-Lending Act is not clear on the question of whether misuse of account numbers constitutes credit card fraud and at least one court has held that fraudulent use of an account number does not constitute the illegal use of a "credit card".[1]

This would be remedied by amending section 134 of the Truth-in-Lending Act and section 916(c) of the Electronic Fund Transfer Act to expand the definition of "credit card" and "debit instrument," respectively. It is not a crime to counterfeit a credit card or to possess such a card, even though counterfeit cards in the hands of a thief can be essentially equivalent to currency (the counterfeiting of which, of course, is illegal). Also, a question has been raised in connection with the $1,000 limit that is contained in several of the subsections of section 134 of the Truth-in-Lending Act and in section 916 of the Electronic Fund Transfer Act. These provisions require that a minimum of $1,000 in money, goods, or services be obtained within a one year period in order to constitute a crime that is punishable under the Federal law. It is not clear whether these subsections require that the government establish only that $1,000 in value has been obtained by credit card fraud or whether the government must show that $1,000 was obtained with a particular counterfeit, lost or stolen card. Arguably a person could use 20 different counterfeit cards to make aggregate purchases of $2,000 but escape liability because no more than $100 was obtained by use of each card. Also, we support the addition of new provisions (section 129 in the Truth-in-Lending Act and section 922 in the Electronic Fund Transfer Act) making it illegal to traffic in account numbers: "(a) with the intent to defraud any consumer or other person; or (b) for any purpose other than a legitimate business purpose involving the . . . account, the [cardholders] [account holders], or the operation of the . . . less system."

The "legitimate business purpose" test has its genesis in the Federal Fair Credit Reporting Act and, since 1970, has been successfully interpreted by administrative agencies and the courts. It would serve the same function here.

Therefore, NRMA supports the provisions recommended by the financial community that would address these problems (see Appendix B to the Statement of the American Bankers Association presented on May 18, 1983).

Given the interstate nature of today's evolving nationwide payments system and the interstate nature of significant fraud cases, we recognize that this situation may warrant a federal response. This is reinforced by the fact that much of the recent increase in credit-related fraud can be attributed to organized crime or, at least, to a criminal element that is highly sophisticated. For these reasons, we believe that Title 18 of the Criminal Code should be revised to include a comprehensive proscription of credit-related fraud. This will enable Federal enforcement authorities to deal effectively with interstate credit-related fraud, including the manufacturing, counterfeiting or altering of credit cards and the fraudulent use of payment devices such as debit cards.

We therefore recommend that the Judiciary Committee of both the House and Senate enact a new chapter to the Criminal Code to address fraud in an area where sophisticated criminals have to date developed ways to circumvent the specific provisions of existing criminal laws.

NRMA believes that the current sensitivity to credit-related fraud on the part of industry and the technological steps that are being taken to curb these practices, coupled with the legislative actions described above, provide the best solutions to this problem. We do not believe that legislation which restricts the merchant's ability to disclose account numbers to third parties in business related activities is the way to combat credit-related crime. For this reason, NRMA opposes legislative language such as that contained in H.R. 2885 because that bill includes a broad prohibition against disclosure of account numbers, with limited specified exceptions. NRMA believes that the primary effect of the proposed restrictions on the ability of a merchant or other credit card issuer to disclose account numbers to a third party would be to inhibit legitimate business activity. The industry already has a strong incentive to protect its customers' account numbers and, as noted, currently is working to improve its anti-fraud technology. In view of the fact that consumers have essentially no liability for fraud losses under the Truth-in-Lending Act, merchants and other credit card issuers understand that they must keep credit card account numbers as confidential as possible.

The industry also has a self-interest in maintaining the confidentiality of this important proprietry information for competitive reasons. There are, however, a number of areas in which account information must be disclosed in connection with the legitimate business needs of the merchant. For example, account information and account numbers are disclosed to institutions acting as merchant banks for retailers, to independent authorization services and to members of the Visa and MasterCard system, to those involved in processing sales slips between banks and merchants, to attorneys and third party debt collectors in connection with the collection of delinquent accounts, to credit bureaus and to other creditors in connection with account verification, and in connection with the marketing efforts that are vitally important to merchants and other credit card issuers. Merchants may also disclose account information to their licensees, to companies engaged in joint ventures with the merchant, and to related companies such as a subsidiary in order to provide the cardholder with an opportunity to purchase new products or services.

---

[1] UNITED STATES v. CALLIHAN, 666 F.2d 422 (9th Cir. 1982).

These examples give some indication of the complexity involved in specifying with completeness and accuracy all of the legitimate business reasons for the communication of account information. The importance of the merchant's ability to use and communicate account information for legitimate business purposes cannot be overemphasized. Any legislative effort to list the permissible uses of account information, and to bar all other uses, is frought with problems and, we believe is the wrong approach to fighting credit card fraud. Account numbers are used in so many facets of the merchant's legitimate business that such legislation would inevitably disrupt and unfairly restrict the merchant's operations. We are convinced that the better approach is to close loopholes in existing criminal statutes and, after careful study by the Judiciary Committees of the House and Senate, possibly enact new provisions to the Criminal Code to combat the recent upsurge in credit-related fraud.

In closing, it is essential that there be a clear demarcation between legislation designed to restrict criminal fraud activities and efforts to restrict account information by legitimate businesses. Any possible problems in the latter area, such as the allegedly excessive solicitations for a credit card registration service that was experienced in Florida recently, can and should be addressed by working within the context of existing laws. Such activities are reprehensible, but they should not be the basis for imposing sweeping industry-wide restrictions on the dissemination of account information by credit card issuers. Legislation should be directed at those who transfer the information with intent to defraud or for purposes other than legitimate business purposes. While we support that kind of legislation, we are strongly opposed to any legislation which would limit the communication of account information for legitimate business purposes.

NRMA commends the Subcommittee for its concern with the serious problem of credit card fraud and appreciates the opportunity to express its views on this subject.

○